DEPARTMENT OF THE AIR FORCE

WASHINGTON, DC

OFFICE OF THE SECRETARY

AFI17-130_AFGM2018-01

19 March 2018

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM SAF/CIO A6
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Air Force Guidance Memorandum to Air Force Instruction 33-200, *Air Force Cybersecurity Program Management*

By Order of the Secretary of the Air Force, this Guidance Memorandum articulates direction to enforce Air Force personnel and contractor compliance with cybersecurity policies and standards. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications; the information herein prevails in accordance with Air Force Instruction 33-360, *Publications and Forms Management*.

As a result of the publication of Air Force Policy Directive 17-1, *Information Dominance Governance and Management*, which supersedes Air Force Policy Directive 33-2, *Information Assurance (IA) Program*, dated 3 August 2011, Air Force Policy Directive 33-200 is hereby renumbered as Air Force Instruction 17-130, *Cybersecurity Program Management*.

Unless otherwise noted, the Secretary of the Air Force Chief, Information Dominance and Chief Information Officer (SAF/CIO A6) is the waiver authority to policies contained in this Air Force Guidance Memorandum. Ensure that all records created as a result of processes prescribed in this publication are maintained as evidentiary documents supporting annual financial audits, or otherwise maintained and disposed of in in accordance with Air Force Manual 33-363, *Management of Records*, and the Air Force Records Disposition Schedule located in the Air Force Records Information Management System.

Air Force Information Technology (defined as traditional Information Technology, Operational Technology, and Platform Information Technology) user's behaviors are monitored to detect potentially unauthorized activity, and punitive methods and procedures will be applied in cases where Air Force uniformed, civilian, or contractor personnel are found in violation of applicable cybersecurity laws, policies and/or standards. **Failure to observe the prohibitions and**

mandatory provisions of this instruction as stated in Attachment 2 by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ),* Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action in accordance with AFI 36-703*, Civilian Conduct and Responsibility,* without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel may be handled according to applicable laws and the terms of the contract. Additionally violations of Attachment 2 by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

This Memorandum describes the role and authorities of the Air Force Chief Information Security Officer in overseeing and managing the Air Force Cybersecurity Program, and bring this Program into alignment with the Presidentially-mandated National Institute for Standards and Technology *Cybersecurity Framework.* This guidance has been incorporated into the upcoming publication Air Force Instruction 17-130, *Cybersecurity Program Management.*

This Memorandum becomes void after one-year has elapsed from the date of this Memorandum, or upon publication of an Interim Change or rewrite of the affected publication, whichever is earlier.

The following guidance applies:

1. General Information

1.1. Introduction

1.1.1. The Air Force Cybersecurity Program aligns with the National Institute for Standards and Technology *Cybersecurity Framework*, and recognizes that risk management and cybersecurity are not static activities, but represent a dynamic, multi-disciplinary set of challenges.

1.1.2. The Air Force Cybersecurity Program encompasses the following functions:

1.1.2.1. *Identify*: Developing and maintaining the organizational understanding required to manage cybersecurity risk.

1.1.2.2. *Protect*: Implementing controls to ensure the delivery of mission critical infrastructure services.

1.1.2.3. *Detect*: The ability to detect cybersecurity events when they occur.

1.1.2.4. *Respond*: The ability to take action regarding detected cybersecurity events.

1.1.2.5. *Recover*: The ability to remain operationally resilient, and to restore capabilities or services that were impaired due to cybersecurity events.

2. Responsibilities

2.1. SAF/CIO A6

2.1.1. In accordance with Air Force Mission Directive 1-26, *Chief, Information Dominance and Chief Information Officer*, appoint an Air Force Chief Information Security Officer to:

2.1.1.1. Direct and oversee the Air Force Cybersecurity Program, including development, oversight and enforcement of policies and standards required to manage entity-wide Air Force cybersecurity risk, as defined in National Security Presidential Directive-54/Homeland Security Presidential Directive 54/-23, *Cybersecurity Policy*, and to implement and enforce the Risk Management Framework in accordance with DoD Instruction 8510.01, *Risk Management Framework (RMF) for Department of Defense Information Technology (IT)* **(T-0)**.

2.1.1.2. Develop and execute an Air Force Continuous Monitoring Strategy.

2.1.1.3. Support and coordinate with other Secretary of the Air Force (SAF)/Headquarters Air Force (HAF) codes as necessary to develop guidance needed to operationalize Air Force cybersecurity.

2.1.1.4. Represent the SAF/CIO A6 cybersecurity interest to all Air Force-internal organizations, and all Federal, State, tribal, and local government agencies. **(T-2)**.

2.1.1.5. Represent the Air Force cybersecurity interest in the planning, programming, budget and execution process. **(T-2)**.

2.1.1.6. Provide Air Force Enterprise oversight of the Air Force Information Technology Asset Management program. **(T-2).**

2.2. Air Force Chief Information Security Officer (SAF/CIO A6Z CISO)

2.2.1. Function as the cyber representative to the Air Force Risk Executive, defined in Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*. In this capacity,

2.2.1.1. Ensure that cybersecurity risk-related considerations are viewed from an Air Force-wide perspective with regard to the Air Force's core missions.

2.2.1.2. Ensure that cyber risk is managed in a consistent manner across the Air Force enterprise reflecting established risk tolerance levels, and considered alongside other Air Force organizational risks.

2.2.1.3. Assist SAF/CIO A6 with carrying out responsibilities enumerated in 10 United States Code 2224, Defense Information Assurance Program, and DoD Instruction 8500.01, *Cybersecurity*. **(T-0)**.

2.2.2. Develop, direct and provide oversight of the Air Force Cybersecurity Program execution; oversee and enforce the execution of this Instruction. **(T-0)**.

2.2.2.1. Serve as the principal advisor to the SAF/CIO A6 on all matters pertaining to cybersecurity, including cyber risk assessment, cyber risk management, cybersecurity budgets and acquisition, and information technology asset management. **(T-1)**.

2.2.2.2. Develop and execute an Air Force risk management strategy. Govern all Air Force risk assessment and risk management activities. **(T-1)**.

2.2.2.3. Develop, promulgate, oversee and enforce cybersecurity policies and standards for all current and proposed Air Force information technology systems, coordinating with other SAF/HAF offices as necessary to develop guidance needed to operationalize the Air Force Cybersecurity Program, and to implement and enforce the Risk Management Framework in accordance with Air Force Instruction 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*. **(T-0)**.

2.2.2.4. Review and approve Cybersecurity Strategies for Air Force information technology systems in accordance with DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, and Air Force Manual 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*; the approval of the Cybersecurity Strategies cannot be delegated. This authority excludes any Air Force information technology system designated as Acquisition Category *ID*, Acquisition Category *IAM* and Acquisition Category *IAC*; Cybersecurity Strategies for systems designated as such must be approved by the Department of Defense Chief Information Officer, in accordance with DoD Instruction 5000.02, *Operation of the Defense Acquisition System*. **(T-0)**.

2.2.2.5. Establish and enforce cyber risk tolerance baselines for Air Force information technology and oversee their enforcement. **(T-1)**.

2.2.2.5.1. In coordination with the SAF/CIO A6 and Authorizing Officials, provide guidance to organizations on how to implement solutions for operational requirements and remain within established risk tolerance baselines. **(T-1)**.

2.2.2.5.2. Ensure that Air Force information technology systems are assigned to and governed by the Air Force Cybersecurity Program. **(T-1)**. Approve National Security System designations for Air Force Information Technology.

2.2.2.5.3. Adjudicate information technology determinations, in coordination with the Air Force Risk Management Council, when there is a conflict in the information technology determination process. **(T-2)**.

2.2.3. On behalf of the SAF/CIO A6, assist with executing Chief Information Officer responsibilities articulated in Air Force Manual 17-1203, *Information Technology Asset Management*. Ensure that organization-wide solutions that support cybersecurity objectives are consistent with Air Force enterprise and security architecture and policy, meet Air Force organizational requirements, and minimize operations and maintenance burdens. **(T-1)**.

2.2.4. Coordinate with and provide advice as required to the Department of Defense Chief Information Security Officer to assist with managing and executing Air Force cybersecurity and Cybersecurity Program activities. **(T-0)**.

2.2.5. Oversee and direct cybersecurity coordination for joint or Defense-wide programs that are deploying information technology (guest systems) to Air Force enclaves. **(T-0)**.

2.2.6. Oversee and direct compliance-related cybersecurity related matters:

2.2.6.1. Oversee and direct activities related to SAF/CIO A6 responsibilities with reference to Public Law 113-283, the *Federal Information Security Modernization Act of 2014 (FISMA)*, 44 United States Code § 3551, et seq. **(T-0)**.

2.2.6.2. Oversee and direct the collection and reporting of cybersecurity management, financial, and readiness data to meet Department of Defense cybersecurity and Office of Management and Budget reporting requirements. **(T-0)**.

2.2.7. Represent the SAF/CIO A6 cybersecurity interests in budget and acquisition processes.

2.2.7.1. Advocate for cybersecurity funding and manning with the Office of the Secretary of Defense and Congress. **(T-1)**.

2.2.7.2. Advocate for Air Force-wide cybersecurity solutions and provide guidance and oversight in the development, submission, and execution of the Air Force cybersecurity program budget through the planning, programming, budget and execution process. **(T-1)**.

2.2.7.3. Oversee and direct any associated budgets and advocate for Air Force-wide cybersecurity solutions through the planning, programming, budget and execution process on behalf of the SAF/CIO A6 in accordance with DoD Instruction 8500.01, DoD Instruction 8510.01, Air Force Policy Directive 17-1, *Information Dominance Governance and Management*, and Air Force Instruction 17-101. **(T-0)**.

2.2.7.4. Coordinate with the Air Force Operational Test and Evaluation Center to ensure cybersecurity testing and evaluation is integrated into the Air Force acquisition process in accordance with Air Force Operational Test and Evaluation Center Manual 99-101, *Operational Test Processes and Procedures,* Air Force Operational Test and Evaluation Center Pamphlet 99-104, *AFOTEC Operational Suitability Test and Evaluation Guide*, and other Air Force Operational Test and Evaluation Center policies and guidance as applicable. **(T-2)**.

2.2.7.5. Validate and prioritize, with the support of the Air Force Risk Management Council, all Air Force cryptographic certification requests prior to submission for National Security Agency action. **(T-0)**.

2.2.7.6. Facilitate the management and implementation identity and access management processes and procedures in accordance with the *DoD Identity and Access Management Strategy*, Version 1.0, October 17, 2014. Review and provide input to Department of Defense Public Key Infrastructure certificate policies. Review and approve Air Force Public Key Infrastructure certificate policies.

2.2.8. Lead and manage key Air Force cybersecurity related bodies:

2.2.8.1. Chair the Air Force Risk Management Council. **(T-2)**.

2.2.8.2. Chair the Air Force Authorizing Official Summit; **(T-1)**.

2.2.8.3. Establish and oversee a Defense Industrial Base Cyber Security/Information Assurance Program Office. **(T-1)**.

2.2.8.4. Appoint Air Force members to the Department of Defense Risk Management Framework Technical Advisory Group. **(T-2)**.

2.2.8.5. Serve as the Air Force representative to the Department of Defense Identity Protection Senior Management Coordinating Group and as the Air Force Public Key Infrastructure Policy Management Authority.

2.2.9. Develop, promulgate and institutionalize an Air Force Continuous Monitoring Strategy. Assess, procure, and implement automated tools and processes to facilitate the measurement and collection of data against defined risk metrics. Provide an enterprise-level cybersecurity common operating picture to inform Air Force-wide risk management decision-making. **(T-1)**

2.2.9.1. Develop guidance regarding how cybersecurity metrics are determined, established, defined, collected, and reported. **(T-1)**.

2.2.9.2. Oversee and direct the collection and reporting of cybersecurity performance measures and metrics to identify enterprise-wide cybersecurity trends and status of mitigation efforts. **(T-1)**.

2.2.9.3. Oversee and direct the process through which cybersecurity metrics are collected and reported for compliance with statutory, Department of Defense, Joint, and Air Force policies and directives. **(T-1)**. Collect and report cybersecurity metrics in coordination with Air Force Chief, Information Dominance and Chief Information Officer, as required by 44 United States Code § 3545. **(T-0)**.

2.2.9.4. Review and approve Defense Industrial Base Cyber Security/ Information Assurance Cyber Intrusion Damage Assessments (as needed) in accordance with DoD Instruction 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA)*. **(T-0)**.

2.2.10. Continuously coordinate and collaborate with National Institute for Standards and Technology and authorities in the Office of the Secretary of Defense on cybersecurity-related issuances. **(T-1)**.

2.2.10.1. Inform Headquarters United States Air Force, and Air Force Major Commands about changes to Department of Defense and Air Force cybersecurity policies and procedures in accordance with Air Force Mission Directive 1-26. **(T-0)**.

2.2.11. In accordance with Air Force Policy Directive 17-1, coordinate as required with the following Staff Codes:

2.2.11.1. Support and coordinate with The Assistant Secretary of the Air Force (Acquisition) (SAF/AQ) to integrate cybersecurity concepts into the Air Force acquisition process. **(T-1)**.

2.2.11.2. Support and coordinate with the Assistant Secretary of the Air Force for Financial Management and Comptroller with achieving and maintaining compliance with Undersecretary of Defense (Comptroller) *Financial Improvement and Audit Readiness (FIAR) Guidance*; ensure that implemented cybersecurity controls, process guidance, and Risk Management Framework assessment documentation support information technology audit inquiries to the greatest degree practicable. **(T-0)**.

2.2.11.3. Support and coordinate with the Deputy Chief of Staff / Manpower & Personnel (HAF/A1) to ensure that personnel security and cybersecurity training policies and standards reflect relevant Cybersecurity Program guidance. **(T-0)**.

2.2.11.4. Support and coordinate with the Deputy Chief of Staff / Intelligence, Surveillance and Reconnaissance (HAF/A2) to ensure that Cybersecurity Program guidance and risk monitoring activities reflect and support Intelligence Community guidance, and that threat and vulnerability data provided by HAF/A2 are integrated into Cybersecurity Program guidance. **(T-0)**.

2.2.11.5. Support and coordinate with the Deputy Chief of Staff / Operations, Plans and Requirements (HAF/A3) to ensure that Air Force Cybersecurity Program policies, standards and activities are consistent with and support the execution of Air Force's five core missions, and that mission risk information and priorities provided from HAF/A3 are used to inform real-time risk management decisions and activities. **(T-0)**.

2.2.11.6. Support and coordinate with the Deputy Chief of Staff / Logistics, Installations and Mission Support (HAF/A4) to ensure that mission assurance information and priorities provided from Deputy Chief of Staff / Logistics, Installations & Mission Support are used to inform real-time risk management decisions and activities. **(T-1)**.

2.3. **Secretary of the Air Force/Headquarters Air Force Functional Leads**

2.3.1. Assist the SAF/CIO A6Z CISO with managing Air Force cyber risk in accordance with the duties and responsibilities presented in Air Force Mission Directive 1-26 and Air Force Policy Directive 17-1. **(T-1)**.

3. Background

3.1. **Cybersecurity Support to Air Force Missions**

The Air Force is organized to address all Mission Areas as authorized and described in DoD Instruction 8115.02, *Information Technology Portfolio Management Implementation*. Air Force support for DoD Mission Areas is accomplished through both administrative and operational Capabilities, which are composed of a wide range of equity interests and functions. While cybersecurity is a key enabler of all Air Force missions and capabilities, information technology is viewed in various ways by different equity interests. The Air Force Cybersecurity Program recognizes the orthogonal nature of the many viewpoints on cybersecurity, along with their relationship to level of command and mission imperative, and is designed to address these viewpoints through an open, flexible cybersecurity framework developed by the National Institute for Standards and Technology.

4. Cybersecurity Program Implementation

4.1. **The Air Force Cybersecurity Program:**

4.1.1. Exists to enable more efficient and effective execution of Air Force's five core missions: air and space superiority; intelligence, surveillance, and reconnaissance; rapid global mobility; global strike; and command and control in and through cyberspace.

4.1.2. Derives its authority from Air Force Mission Directive 1-26 and Air Force Policy Directive 17-1.

4.1.3. Adopts the National Institute for Standards and Technology Cybersecurity Framework as its basis; all Air Force information technology systems' cybersecurity programs must fully address the Framework's five Functions.

4.1.4. Recognizes that risk management is not a static activity; risk management technologies, processes and practices must continuously evolve and improve to match the ever-changing threat environment.

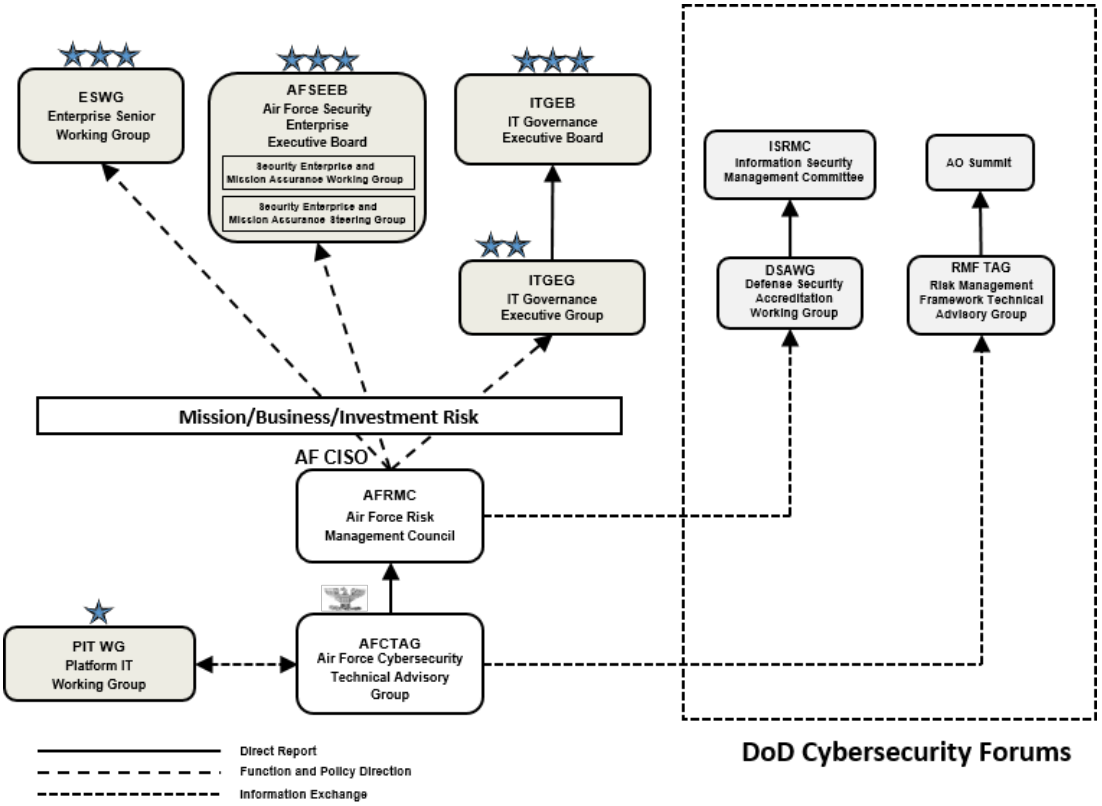
4.2. **Identify**

The Air Force Cybersecurity Program addresses the Framework Identify Function by developing and evolving Air Force's understanding of how to effectively manage cybersecurity risk to Air Force systems, assets, data, and capabilities. Air Force leaders and managers must continuously strive to maintain an understanding of cybersecurity in the mission/business context, the resources that support critical functions, and the related cybersecurity risks, with the goal of enabling Air Force to focus and prioritize its efforts, consistent with its risk management strategy and mission/business needs.

4.2.1. **Business Environment.** The Air Force exists to perform the five core missions described in section 4.1.1, and thus the principal Air Force Cybersecurity Program goal is to manage cyber risks down to a level that enables and supports Air Force success in executing those missions, rather than to eliminate risk.

4.2.2. **Governance.** Cybersecurity governance occurs at all levels of the Air Force enterprise and ensures cybersecurity strategies are aligned with mission and business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility. The Air Force Cybersecurity Governance Structure (Figure 4.1) uses Air Force and Department of Defense corporate boards and processes to help ensure that risk management topics are raised to the appropriate level, and that informed decisions can be made to manage Air Force cybersecurity risk.

Figure 4.1. Air Force Cybersecurity Governance.



Air Force Cybersecurity Program governance and oversight mechanisms include:

4.2.2.1. *Governance Processes*. The governance process must ensure Federal Information Security Modernization Act, Department of Defense, and Air Force cybersecurity policy compliance, requiring senior agency officials to provide security for information and information systems that support the operations and assets under their control.

4.2.2.2. *Governance Bodies*. The Air Force will leverage existing Air Force and Department of Defense governance bodies (shaded boxes of Figure 4.1— Air Force Security Enterprise Executive Board, Information Technology Governance Executive Board, Information Technology Governance Executive Group, Enterprise Security Working Group, etc.) to discuss cybersecurity risk topics and make organizational and mission/business area risk decisions. This Instruction does not define the scope or responsibilities of these existing bodies.

4.2.2.3. *Cybersecurity Policy*. Air Force will develop, update, promulgate, oversee and enforce risk management policies and standards that translate Air Force missions, goals and strategic plans into actionable directives. These policies will also assign responsibilities and delegate authorities that are coordinated and aligned with internal roles and external partners.

4.2.3. **Risk Management Strategy.** The Air Force Cybersecurity Program's Risk Management Strategy must:

4.2.3.1. Ensure that the confidentiality, integrity, and availability of all information owned or held in trust by the Air Force is protected with in accordance with the requirements of Air Force Instruction 17-101 and/or applicable law or policy. **(T-0)**.

4.2.3.2. Be integrated into all key mission and business processes; e.g., the Operational Security process as defined in Air Force Instruction 10-701, *Operations Security (OPSEC).* **(T-1)**.

4.2.3.3. Promote and support operational agility. Pursuant to the requirements articulated in section 4.2.5, cybersecurity capabilities will be acquired, implemented and operated in a manner that maximizes performance, while enhancing safety, reliability, interoperability, and ease of use. The cost and use of cybersecurity capabilities must be continuously balanced against the likelihood of data loss or corruption and the associated mission impacts. **(T-1)**.

4.2.3.4. Promote transparency and interoperability with Air Force mission partners:

4.2.3.4.1. Air Force documentation regarding the design and effectiveness of controls will be made available to all mission partners in furtherance of reciprocity, as described in DoD Instruction 8510.01. **(T-0).**

4.2.3.4.2. Cybersecurity capabilities that are shared between Air Force and other mission partners will be governed and managed in accordance with guidance contained in DoD Directive 8000.01, *Management of the Department of Defense Information Enterprise (Department of Defense IE)*. **(T-0).**

4.2.4. **Risk Assessment.** Air Force Cyber risk will be managed deliberately through formal and regularly executed processes and measurements:

4.2.4.1. The Risk Management Framework will be leveraged to help manage risk across all Air Force Information Technology; all Air Force systems will implement the Risk Management Framework in accordance with Air Force Instruction 17-101. **(T-1)**.

4.2.4.2. Risk will be subjected to continuous monitoring at all command levels. Organizations subject to the authority of this Instruction will regularly review audit scans on their networks and network-connected devices in accordance with guidance contained in DoD Instruction 8530.01, *Cybersecurity Activities to Support DoD Information Network Operations,* to detect inappropriate configurations and malware. **(T-0)**.

4.2.4.3. Air Force Cybersecurity Program performance will be measurable and auditable; metrics concerning the design and effectiveness of cybersecurity controls on Air Force information technology systems will be developed and systematically collected in accordance with guidance contained in Chairman, Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND),* **(T-0)**, and Air Force Manual 17-2101, *Long-Haul Communications Management*. **(T-1)**, and reported up to SAF/CIO A6Z CISO leadership:

4.2.4.4. Collected metrics will be analyzed to gain an understanding of the relationship between the design and effectiveness of controls against Air Force strategic goal achievement and core mission effectiveness. **(T-1)**.

4.2.4.5. Cybersecurity performance data will be collected throughout all Air Force information technology systems' lifecycles. **(T-1)**.

4.2.5. **Asset Management.** The Air Force Cybersecurity Program will promote flexible and resilient Air Force system capabilities. Air Force information technology systems must be planned, developed/acquired, tested, implemented, operated and monitored to ensure that:

4.2.5.1. All Air Force hardware, software and firmware that are connected to Air Force networks and/or which process, store, or transmit information owned or held in trust by Air Force are registered and entered into inventory and tracked throughout their lifecycles. Non-Air Force hardware, software and firmware that are connected to Air Force networks and/or which process, store, or transmit information owned or held in trust by Air Force must receive formal approval prior to connection, as defined in 4.2.5.2 or through the completion of the assess-only Risk Management Framework process defined in Air Force Instruction 17-101. **(T-1)**.

4.2.5.2. Air Force organizations requiring a connection to the Defense Information System Network, including the Non-Secure Internet Protocol Router Network, Secure Internet Protocol Router Network, and the Department of Defense Cloud, must adhere to the Defense Information Systems Agency Connection Approval Process; Chairman, Joint Chiefs of Staff Instruction 6211.02D, *Defense Information Systems Network (DISN) Responsibilities*, is germane. Defense Information System Network and Department of Defense Cloud Connection Process Guides are published by Defense Information Systems Agency, and may be downloaded from the following Non-secure Internet Protocol Router Network link:

http://www.disa.mil/connect

4.2.5.3. Air Force organizations requiring a connection to the Air Force Information Network or Air Force Network must comply with the connection approval guidance provided in Air Force Instruction 17-101. **(T-1)**.

4.2.5.4. Air Force organizations requiring a connection (wired or wireless) to non-Air Force or non-Department of Defense networks, web servers, services, applications, or capabilities must comply with the connection approval guidance provided in Air Force Instruction 17-101, and the security requirements in Air Force Manual 17-1301, *Computer Security (COMPUSEC)*. **(T-2)**.

4.2.5.4.1. Mobile air cards and/or mobile hotspots for Temporary Duty/mobile usage do not require a Commercial Internet Service Provider waiver, however, approved devices and mobile data service must be obtained through Information Technology Commodity Council-approved contracts. **(T-0)**.

4.2.5.4.2. Such devices and services must not be used as permanent substitutions for office Information Technology. **(T-2)**.

4.2.5.4.3. Mobile hotspots and devices must be configured in accordance with applicable Defense Information Systems Agency *Wireless* Security Technical Implementation Guides. **(T-2)**.

4.2.5.4.4. Encryption solutions must be selected from among those that are approved (e.g. Cisco Virtual Private Network Client, Juniper Network Connect, Citrix). **(T-0)**.

4.2.5.4.5. Organizations that use Department of Defense devices that attach to the Non-secure Internet Protocol Router Network via these means must ensure they connect through a Virtual Private Network first. Refer to Defense Information Systems Agency Security Technical Implementation Guides for use of mobile hotspot feature on Commercial Mobile Devices/smartphones. **(T-0)**.

4.2.5.5. Air Force cybersecurity assets that feature ease of maintenance are preferred; to the greatest extent practicable, Air Force information technology systems are designed/procured to be self-defending and self-healing, requiring little or no manual intervention, and maintain an audit trail of all such actions. **(T-3)**.

4.2.5.6. Air Force cybersecurity assets will be acquired, implemented and operated in a manner that maximizes performance, while enhancing safety, reliability, interoperability, and ease of use. The cost and use of cybersecurity capabilities must be continuously balanced against the likelihood of data loss or corruption and the associated mission impacts. **(T-2)**.

4.2.5.7. The security posture/status of Air Force cyber capabilities and resources, from individual systems through aggregated capabilities, is visible to and trustable by managers, users, and mission partners. **(T-1)**.

4.2.5.8. Air Force cyber assets and capabilities are managed to ensure that systems and data are available when and where needed; all resources are prioritized based on their classification, mission criticality, and business value. **(T-1)**.

4.2.5.9. Air Force Cyber Workforce and baseline cybersecurity training for all Air Force military, civilian and contract employees is continuously overseen and monitored. **(T-1)**.

4.3. Protect

The Air Force Cybersecurity Program serves the Framework's *Protect* function by designing, implementing, and continuously monitoring the effectiveness of controls, executing risk assessment and management processes and procedures:

4.3.1. **Access Control.** Subjects' (humans, applications) access and privileges to manipulate objects (data, files) will be controlled in a manner consistent with mission requirements and security needs, and in accordance with Department of Defense 5220.22-M, **(T-0)**, this Instruction, and Air Force Manual 17-1301. **(T-2)**. Access permissions must be actively managed and monitored through each authorized account's lifecycle, incorporating the principles of least privilege and separation of duties. **(T-1).**

4.3.1.1. All Air Force information technology systems must employ mechanisms to monitor and control access, with the purpose of limiting access to users and subjects that

have been formally granted access permissions. **(T-1)**. See also section 4.3.6, Protective Technologies.

4.3.1.2. Strong authentication mechanisms must be employed. **(T-1)**.

4.3.1.3. Anonymous access by person (i.e., human) subjects must be disallowed. Technical solutions to address 24/7, multi-user, operational systems must be implemented to ensure personal accountability while simultaneously addressing operational continuity requirements. **(T-1)**.

4.3.1.4. In accordance with Air Force Instruction 10-712, *Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process*, all Air Force information technology must comply with installation certification procedures, to include notice and consent certification requirements. **(T-1)**.

4.3.1.5. Networks/network operating systems must support the following functionality; external clients must:

4.3.1.5.1. Obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained, using a service providing secure name/address resolution services (e.g., Domain Name Service) . **(T-2)**.

4.3.1.5.2. Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. **(T-2)**.

4.3.1.5.3. Be fault-tolerant and implement internal/external role separation. **(T-2)**.

4.3.1.5.4. Protect the authenticity of communications sessions. **(T-2)**.

4.3.1.6. Systems and networks must be capable of being configured to disconnect network-connected devices after a defined idle period, or upon violation of a defined system security policy (e.g., attempt to exceed role authority, too many failed login attempts, insertion/connection of a prohibited device such as a thumb drive). **(T-1)**.

4.3.1.7. Enclaves must be architected to provide for boundary protections and managed interfaces featuring layered physical and logical protections. **(T-1)**.

4.3.1.8. Organizational architecture policies and standards must address authorized use of mobile code, mobile devices, collaborative computing devices, and third-party/personally owned hardware and software. Unless explicitly authorized, physical or wireless connection of personally-owned hardware and/or software to Air Force information technology is prohibited. Refer to Attachment 7, Authorized Use of Personally-owned Devices, and Air Force Manual 17-1301 for further guidance. **(T-3)**.

4.3.1.9. Authorized wireless devices and services connected to or capable of connecting to Air Force information technology must comply with DoD Instruction 8500.01 and DoD Directive 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*. **(T-0)**. Refer to Air Force Instruction 17-101 and Air Force Manual 17-1301 for additional information on protections, deployment and support of wireless services. **(T-1)**.

4.3.1.10. Use of storage media that is designed to be plugged into and removed from Air Force information technology is prohibited unless explicitly authorized by cognizant authority. This includes, but is not limited to: external hard drives; optical media (e.g., Compact Disks, Digital Video Disks); flash media (e.g., memory cards, Universal Serial Bus flash drives, and solid-state drives). **(T-1)**.

4.3.1.11. Biometrics used to support identity assurance will be managed in accordance with guidance contained in Chairman, Joint Chiefs of Staff Instruction 6510.01F, and DoD Directive 8521.01E, *Department of Defense Biometrics*. **(T-0)**.

4.3.1.12. Physical access to and physical protection of computing facilities that process publicly releasable, sensitive, or classified information must employ physical security measures (i.e., access control, visitor control, physical control, testing, etc.), that restrict access to only authorized personnel with appropriate clearances and a need-to-know, in accordance with Department of Defense 5200.08-R, Physical Security Program and Department of DefenseM5205.07V3_Air Force Manual16-703V3, *Department of Defense Special Access Program (SAP) Security Manual: Physical Security*. **(T-0)**.

4.3.2. Awareness and Training.

4.3.2.1. All Air Force personnel will achieve and maintain the proper certification in accordance with DoD Directive 8140.01, *Cyberspace Workforce Management*, DoD 8570.01- M and Air Force Manual 17-1303, *Cybersecurity Workforce Improvement Program*, before serving in a cybersecurity-designated billet. **(T-0)**.

4.3.2.2. All Air Force personnel must complete Information Assurance Awareness training prior to system access and annually thereafter. Training will be tracked by the Air Education and Training Command, via the Advanced Distributed Learning System. **(T-1)**. Users who require a new account or modification to an existing account are not required to retake the Department of Defense Cybersecurity training provided the user has a valid and current course completion record.

4.3.3. Data Security.

4.3.3.1. Designed-in Protection Paradigm. All systems and network communications pathways will be managed and protected to an extent consistent with mission requirements, and in accordance with guidance contained in this Instruction, Air Force Instruction 63-101/20-101, *Integrated Life Cycle Management*, Air Force Manual 17-1301 and Air Force Manual 17-1302-O, *Communications Security (COMSEC) Operations*; operating systems, applications, databases and network components must be designed and procured with protection features designed-in **(T-1)**:

4.3.3.1.1. Operating systems must be capable of partitioning applications, isolating processes and security functions, supporting object reuse, managing resource availability through automatic process prioritization. **(T-1)**.

4.3.3.1.2. Internal and external communications modalities and storage media must provide for the protection of information in transit and at rest. Physical and logical protections, including encryption techniques must be used within the proper

management construct; i.e., a process for Public Key Infrastructure certificate and encryption key management. **(T-1)**.

4.3.3.1.3. Data-at-Rest must be protected commensurate to the sensitivity and integrity concerns associated with the data; the principle of encrypt-by-default will be employed as the default configuration whenever possible. In accordance with United States Cyber Command Cyber Tasking Order 08-001, *Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media Used Within the Department Of Defense (DoD)*, and this Instruction, information identified as Controlled Unclassified Information, For Official Use Only, Personally Identifiable Information, and/or Protected Health Information, must be protected by Federal Information Processing Standard 140-2, *Security Requirements for Cryptographic Modules*-compliant encryption while at rest. Refer to Air Force Manual 17-1301 for additional guidance. **(T-0)**.

4.3.3.1.4. Data-in-Transit must be protected commensurate to the sensitivity and integrity concerns associated with the data; all systems that are continuously or periodically connected to networks via a local or remote connection must be capable of supporting link security and data encryption to protect the confidentiality and/or integrity of information in transit. In accordance with United States Cyber Command Cyber Tasking Order 08-001, *Controlled Unclassified Information, For Official Use Only, Personally Identifiable Information*, DoDM 5205.07V3_Air Force Manual 16-703V3, *DoD Special Access Program (SAP) Security Manual Marking*, the *E-Government Act of 2002*, and Office of Management and Budget Memo M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, must be protected by Federal Information Processing Standard 140-2 compliant encryption while in transit. Refer to Attachment 2 and Air Force Manual 17-1301 for additional guidance. **(T-0)**.

4.3.3.2. Controls to prevent unauthorized changes to software, firmware, and information that occur due to errors or malicious activity (e.g., tampering) must be implemented. **(T-1)**. Air Force systems must feature state-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools to automatically monitor the integrity of systems and applications.

4.3.3.3. The integrity of Air Force systems' functions, software, firmware and information must be ensured, including, but not limited to:

4.3.3.3.1. Internal integrity functions such as memory protection, and automated error detection and alerting. **(T-2)**.

4.3.3.3.2. System audit event and attack detection alerts. **(T-2)**.

4.3.3.3.3. Use of external monitoring, scanning, and reporting tools. **(T-2)**.

4.3.3.3.4. Manual post-event review and reconciliation/validation. **(T-2)**.

4.3.3.3.5. Memory protection.

4.3.3.4. Collaborative computing technologies must be sited and configured to prevent unauthorized users from seeing and/or hearing information for which they are not cleared or do not have a need to know. Additionally, safeguards must be implemented to guard against the aggregation of data from various sources that could be classified at a higher level than the Air Force information technology in question is not rated to process, store or transmit. Refer to Air Force Manual 17-1301 for additional guidance. **(T-1)**.

4.3.3.5. Access to media containing Air Force information or information held in trust by Air Force must be controlled, marked, stored and transported in accordance with its sensitivity level and handling instructions; Executive Order13526, *Classified National Security Information*, and Executive Order 13556, *Controlled Unclassified Information*, as amended, Department of Defense Manual 5200.01, Volume 2, *Department of Defense Information Security Program: Marking of Classified Information*, and Volume 4, *Department of Defense Information Security Program: Controlled Unclassified Information (CUI)*, Department of Defense 5400.11-R, *Department Of Defense Privacy Program*, DoD Directive 5400.11, *Department of Defense Privacy Program*, Air Force Instruction 33-332, *The Air Force Privacy and Civil Liberties Program*, et. al., are germane. Physical and logical assets must be handled in accordance with governing guidance during the process of removal, transfer or retirement. **(T-0)**.

4.3.3.6. Media containing Air Force information or information held in trust by Air Force will be disposed of in accordance with DoD Instruction 5015.02, *Department of Defense Records Management Program*, DoDM 5205.07V3_Air Force Manual16-703V3 and Department of Defense 5220.22-M, *National Industrial Security Operations Manual (NISPOM)*, and inventories modified to account for the loss. **(T-0)**.

4.3.3.7. Adequate inventories and or access to replacement assets must be maintained consistent with mission requirements. **(T-1)**.

4.3.3.8. Usage restrictions and implementation guidance for Voice over Internet Protocol technologies must be established based on the potential for malicious damage to systems and operations. **(T-2)**. All Voice over Internet Protocol connections must be authorized, monitored, and controlled. **(T-2)**.

4.3.4. Information Protection Processes and Procedures.

4.3.4.1. Cybersecurity controls to address Air Force and Department of Defense requirements must be a substantial and visible component in Air Force acquisitions in accordance with the requirements of DoD Instruction 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, and Air Force Instruction 63-101/20-101, **(T-0)** and integrated fully within the Air Force acquisition process:

4.3.4.1.1. All Air Force information technology systems' portfolios, contracts, and third-party agreements will make cybersecurity a visible and quantifiable element. Cybersecurity projects across multiple investments will be coordinated using the portfolio management processes defined in Air Force Instruction 17-110, *Air Force Information Technology Portfolio Management and IT Investment Review*. **(T-1)**.

4.3.4.1.2. Air Force acquisition officials will manage supply chain risk in accordance with DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),* and Air Force Pamphlet 63-113, *Program Protection Planning for Life Cycle Management*. **(T-0)**.

4.3.4.1.3. Air Force information technology systems will, to the greatest extent practicable, adhere to Department of Defense and Air Force enterprise architecture principles in accordance with DoD Directive 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE)*, and Air Force Instruction 17-140, *Air Force Architecting*, adopt a standards-based approach, and emphasize risk sharing and balancing to achieve mission success. **(T-0)**.

4.3.4.1.4. All interconnections with Air Force networks and systems will be managed in a manner calculated to minimize shared risk; the cybersecurity posture of one system must not be undermined by weaknesses in other interconnected systems. **(T-1)**.

4.3.4.1.5. Air Force acquisition and cybersecurity personnel will ensure that all Air Force information technology hardware, firmware, and software components or products incorporated into DoD Instruction comply with evaluation and validation requirements contained in DoD Instruction 8500.01 and Committee on National Security Systems Policy 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products* **(T-0)**; when operationally and technically practicable, Program Managers and system engineers/ integrators will prefer Department of Defense-approved products listed in the following sources: **(T-1)**.

4.3.4.1.5.1. Certified TEMPEST Manufacturer Program; (www.iad.gov/iad/programs/iad-initiatives/tempest.cfm)

4.3.4.1.5.2. Department of Defense Unified Capabilities Approved Products List; (https://aplits.disa.mil/)

4.3.4.1.5.3. Air Force Evaluated Products List; (https://cs2.eis.af.mil/sites/10336/lists/cotsgots%20software/epl.aspx)

4.3.4.1.5.4. Common Criteria Evaluation and Validation Scheme; (http://www.commoncriteriaportal.org/products) and (http://www.niap-ccevs.org)

4.3.4.1.5.5. Product Director Automated Movement and Identification Solutions; (http://www.pdamis.army.mil)

4.3.4.1.6. Cybersecurity concerns must be addressed throughout systems' life cycles, beginning with pre-Milestone A capabilities requirement processes and continuously thereafter to Program retirement. DoD Instruction 5000.02, DoD Instruction 5134.16, *Deputy Assistant Secretary of Defense for Systems Engineering (DASD (SE))*, Air Force Instruction 63-101/20-101, and Department of Defense Chief Information Officer/Undersecretary of Defense for Acquisition, Technology and Logistics guidance concerning the approval of multi-factor authentication alternatives, e.g., Rivest Shamir and Adelman and YubiKey, are germane. **(T-0)**.

4.3.4.2. Configuration management processes must be institutionalized and documented throughout Air Force systems' life cycles – see Undersecretary of Defense - Acquisition,

Training and Logistics MIL-HDBK-61A(SE), for further guidance. **(T-1)**. Personnel with cognizance over configuration management processes must ensure that:

4.3.4.2.1. All Configuration Items are identified and memorialized; the Configuration Item list/database itself must be controlled as a Configuration Item. **(T-1)**.

4.3.4.2.2. The development, test and promotion to production of their respective systems are governed by a formal Systems Development Life Cycle process; strict segregation of these environments must be maintained in accordance with Attachment 6, Segregation of Duties and Least Privilege. **(T-1)**.

4.3.4.2.3. The development and modification of system Configuration Items, including software, hardware, firmware, data and files, is governed by a Configuration Control Board that reviews, assesses, and approves at its discretion all proposed changes to Configuration Items **(T-1)**, and ensures:

4.3.4.2.4. That the current, approved collection of Configuration Items is maintained as a formal baseline. **(T-1)**.

4.3.4.2.5. That system-specific change management standards and procedures are developed, approved, promulgated and enforced. **(T-2)**.

4.3.4.2.6. Air Force information technology must be configured to provide only essential capabilities, and prohibit or restrict the use of formally defined/proscribed functions, ports, protocols, and/or services in accordance with DoD Instruction 8551.01, *Ports, Protocols, and Services Management (PPSM),* and Air Force System Security Instruction 8551, *Ports, Protocols, and Services Management (PPSM).* **(T-0)**.

4.3.4.2.7. Security configuration and implementation decisions will be guided by relevant Federal and Department of Defense guidance, such as National Institute for Standards and Technology Special Publications, Defense Information Systems Agency Security Technical Implementation Guides (http://iase.disa.mil/stigs/), and National Security Agency Security Configuration Guides. Guidance will be applied to each Air Force information technology system and enclave to establish and maintain a minimum baseline security configuration and posture in accordance with this Instruction and Air Force Instruction 17-101. **(T-1)**.

4.3.4.2.8. Configuration changes to Air Force information technology CIs must be analyzed and approved by the cognizant configuration and cybersecurity authorities prior to implementation in a production environment. **(T-2)**. Both approved and rejected changes will be formally documented in meeting minutes, and posted in each systems' Risk Management Framework authorization package in accordance with the requirements in Air Force Instruction 17-101. **(T-1)**.

4.3.4.3. A vulnerability management plan consistent with the Cyber Ready 365 initiative must be developed and implemented. **(T-1)**.

4.3.4.4. Plans, processes and standards for reacting to cybersecurity incidents must be developed, approved, and promulgated. **(T-1)**. The following requirements apply:

4.3.4.4.1. Local standards must be developed to define system events or patterns of events that may be classified as an incident. **(T-3)**.

4.3.4.4.2. Incident response plans and procedures must be developed for each Air Force system or enclave that define the incident management, handling, and reporting chain, response procedures, and escalation procedures for incidents that develop into a system continuity event. **(T-3)**. Plans must be exercised/tested on no less than an annual basis. **(T-2)**.

4.3.4.4.3. Performance records and lessons-learned must be memorialized and retained following exercise/test evolutions. **(T-1)**.

4.3.4.4.4. Back-ups of critical software and data files must be regularly conducted, maintained, protected, and periodically tested. **(T-1)**. Local organizational policy dictates frequency and limitation factors. **(T-3)**.

4.3.4.5. Systems must be configured to allow users to create content only at their own sensitivity/security level, and view content only at or below their own sensitivity/security level. Spillages (i.e., creation or posting of information at a higher sensitivity/security level than the Air Force information technology is accredited to process, store, or transmit), must be immediately reported in accordance with local procedures, measures taken to prevent the spread of the spillage, and prompt action to clear or sanitize the effected hardware and software. Refer to Air Force Manual 17-1301 for additional guidance.

4.3.5. **Maintenance.** Cybersecurity controls to address Air Force cybersecurity concerns must be a substantial and visible component in Air Force maintenance contracts and support agreements in accordance with DoD Instruction 4000.19, *Support Agreements*: **(T-0).**

4.3.5.1. All Air Force information technology systems' maintenance contracts and agreements will make cybersecurity a visible and quantifiable element. **(T-1)**.

4.3.5.2. All remote maintenance connections with Air Force networks and systems will be managed in a manner calculated to minimize risk and prevent unauthorized access. **(T-2)**.

4.3.5.3. All maintenance actions must be logged; the date and time of service must be recorded, and the person(s) performing the maintenance action must be identified. All maintenance actions must also be registered in systems as auditable events. **(T-2)**.

4.3.6. **Protective Technology.**

4.3.6.1. In order to ensure accountability and non-repudiation, Air Force will rely on the Department of Defense Public Key Infrastructure Program to access a Public Key Infrastructure that interoperates and is integrated with the Department of Defense Public Key Infrastructure, National Security System Public Key Infrastructure, external federated Public Key Infrastructures and associated identity and access control management technologies in accordance with DoD Instruction 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, and Air Force Manual 17-1301. Public Key Infrastructure will be employed to authenticate subjects, both human and non-person entities, on all Air Force information technology in accordance with DoD Instruction 8520.03, *Identity Authentication for Information Systems*; Platform Information Technology Weapon

Systems will assess Public Key Infrastructure feasibility utilizing risk-based assessments. **(T-0)**.

4.3.6.2. Encryption keys must be managed through a Key Management Infrastructure that provides a framework and services to generate, produce, store, protect, distribute, control, track and destroy all symmetric and asymmetric keying materials and certificates. The Key Management Infrastructure system must provide the means to deliver cryptographic products, key management products and services to a large and diverse community of globally distributed users in accordance with Air Force Manual 17-1302-O. **(T-1)**.

4.3.6.3. Communications security controls will be implemented on all non-public Air Force information technology communications networks to protect information confidentiality, availability, and integrity in accordance with Air Force Manual 17-1302-O, and applicable Department of Defense guidance. **(T-0)**.

4.3.6.4. Air Force information technology will employ validated Federal Information Processing Standard 140-2 cryptographic modules in accordance with the National Institute for Standards and Technology Cryptographic Module Validation Program unless explicitly exempted. **(T-1)**.

4.3.6.5. Public Key Infrastructure solutions will be managed through the Department of Defense Public Key Infrastructure Program Management Office, while specific access certificates will be managed locally by Air Force. The Department of Defense Chief Information Officer guidance concerning the approval of multi-factor authentication alternatives, e.g. Rivest Shamir and Adelman and YubiKey, is also germane. **(T-0)**.

4.3.6.6. Air Force will use hardware tokens, including the Department of Defense Common Access Card, AFNET-S tokens, Alternate Login Tokens, and Volunteer Logical Access Credential, to Public Key Infrastructure-enable Air Force information technology in accordance with DoD Instruction 8520.02, DoD Instruction 8520.03, *Identity Authentication for Information Systems*, and Air Force Manual 17-1301. Platform Information Technology Weapon Systems will assess Public Key Infrastructure feasibility utilizing risk-based assessments. **(T-0)**.

4.3.6.7. Cross Domain Solutions must adhere to the requirements of DoD Instruction 8540.01, *Cross Domain (CD) Policy*.

4.3.6.7.1. The Unified Cross Domain Services Management Office maintains a baseline list of National Security Agency-certified solutions available for reuse contingent on approval by the Defense Information Assurance Security Accreditation Working Group; see the link available through the following Secure Internet Protocol Router Network link:

https://intelshare.intelink.sgov.gov/sites/ucdsmo/default1.aspx

4.3.6.7.2. For guidance on the most current Cross Domain Solution approval process, contact the Air Force Cross Domain Support Element, and consult the Defense Information Systems Agency Mission Partners website at the following Non-secure Internet Protocol Router Network link:

http://disa.mil/Services/Network-Services/Enterprise-Connections/Mission-Partner-Training-Program.

4.3.6.7.3. Send all requests for Cross Domain Solutions and coalition information sharing solutions to the following Non-secure Internet Protocol Router Network link:

https://intelshare.intelink.gov/sites/afcdse/SitePages/Home.aspx

4.3.6.8. All Air Force information technology must implement TEMPEST protections to mitigate vulnerabilities resulting from radio frequency emanations from such systems in accordance with Air Force System Security Instruction 7702, *Emission Security Countermeasures Reviews*. Personnel assigned to duties that involve TEMPEST management or implementation must be qualified in accordance with Air Force System Security Instruction 7702 requirements. **(T-2)**.

4.3.6.9. Collaborative computing (video teleconferencing, etc.) aids in mission accomplishment by providing a means for groups and/or organizations to share and relay information. However, the cognizant Information System Security Officer should be contacted for guidance on connecting video cameras and microphones to Air Force Information Technology.

4.3.6.10. Organizations subject to the authority of this Instruction will regularly review results of audit scans on their information technology systems in accordance with guidance contained in DoD Instruction 8530.01 to detect inappropriate configurations and malware. **(T-1)**.

4.3.6.11. Cybersecurity Program performance will be measurable and auditable; metrics concerning the design and effectiveness of cybersecurity controls on Air Force information technology systems will be developed and systematically collected in accordance with guidance contained in Chairman, Joint Chiefs of Staff Instruction 6510.01F, and Air Force Manual 17-2101, *Long Haul Communications Management*, and reported up to SAF/CIO A6Z CISO leadership **(T-0)**:

4.3.6.11.1. Collected metrics will be analyzed to gain an understanding of the relationship between the design and effectiveness of controls against Air Force strategic goal achievement and core mission effectiveness. **(T-1)**.

4.3.6.11.2. Cybersecurity performance data will be collected, analyzed, and reported to the cognizant Authorizing Official, and summarized for the Chief Information Security Officer throughout all Air Force information technology systems' lifecycles. **(T-1)**.

4.4. Detect

The Air Force Cybersecurity Program addresses the Framework *Detect* Function through the design and/or implementation of Air Force procured or Department of Defense-provided, enterprise-wide automated tools/solutions (e.g., Host Based Security System) or tools/solutions that are developed in accordance with Department of Defense data exchange/data sharing standards (e.g., National Institute for Standards and Technology, Security Content Automation Protocol, Department of Defense Metadata Directory, etc.) to ensure interoperability with

enterprise-wide solutions for the discovery and analysis of undesirable events and for remediation of vulnerabilities

4.4.1. **Monitoring Warnings.** Users of Department of Defense telecommunications devices are to be notified the use of these systems constitutes consent to monitoring. **(T-1).**

4.4.1.1. All users of Department of Defense information systems will sign a standardized User Rules of Behavior Agreement. **(T-2)**. Local organizational commanders must restrict access to Air Force Information Technology for those personnel who fail to sign the agreement. **(T-3)**. Organization Information System Security Officers are required to report to the Enterprise Service Desk any failures to sign the agreement for revocation of access to enterprise capabilities. **(T-1)**.

4.4.1.2. To maintain continuous notifications to all users using Air Force or Department of Defense telecommunications devices including Voice over Internet Protocol phone instruments, users will report to the Information System Security Officer any of following deficiencies **(T-3)**:

4.4.1.2.1. A DD Form 2056, Telephone Monitoring Notification Decal, is missing or not readable on the front of all official telephones and VoIP phone instruments. **(T-3)**.

4.4.1.2.2. A DD Form 2056 is missing or not readable on fax machines. **(T-3)**.

4.4.1.2.3. Locally created organizational/unit fax cover sheets do not contain the exact notice and consent statement: *"Do not transmit classified information over unsecured telecommunications systems. Official Department of Defense telecommunications systems are subject to monitoring. Using Department of Defense telecommunications systems constitutes consent to monitoring."* **(T-3)**.

4.4.2. **Anomalies and Events.** Air Force system and network owners must gain an understanding of what "normal" looks like by establishing and managing a baseline profile of nominal operations, expected data flows, and undesirable/anomalous events (clipping levels). Events that exceed clipping level thresholds will be treated as potential incidents, and in accordance with the guidance contained in DoD Instruction 8530.01 and Air Force issuances cited below. **(T-0).**

4.4.2.1. Continuous Monitoring. Risk will be viewed as a dynamic problem set, requiring continuous monitoring to manage effectively. **(T-1)**.

4.4.2.2. Air Force networks will implement/leverage Department of Defense Endpoint Security Solutions, (i.e., Host Based Security System), engineering and architecture services), to detect, deter, protect, and report on cyber threats across Air Force networks. **(T-1)**.

4.4.2.3. Connection to Air Force networks by unauthorized devices (e.g., thumb drives, external hard drives) must be automatically detected and isolated. **(T-1)**.

4.4.2.4. Physical and environmental controls commensurate to the risk environment must be implemented and monitored to detect and rapidly respond to threats, in accordance with

Air Force Policy Directive 16-14, *Security Enterprise Governance*, and subordinate guidance. **(T-1)**.

4.4.2.5. User's behaviors are monitored to detect potentially unauthorized activity. **Failure to observe the prohibitions and mandatory provisions of this instruction as stated in Attachment 2 by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action in accordance with AFI 36-703, *Civilian Conduct and Responsibility*, without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel may be handled according to applicable laws and the terms of the contract. Additionally violations of Attachment 2 by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. (T-0)**.

4.4.2.6. Air Force information technology will be protected from threats associated with unauthorized or improper use of mobile code in accordance with the requirements in DoD Instruction 8500.01, and Air Force Manual 17-1301. **(T-0)**. Acceptable and unacceptable mobile code technologies, usage restrictions, and implementation guidance will be defined for each Air Force information technology system. **(T-1)**. Acceptable mobile code use must be explicitly authorized, monitored, and controlled. System developers and implementers must adhere to the guidance contained in all applicable Security Technical Implementation Guides during system acquisition and fielding. **(T-0)**.

4.4.2.7. Anti-malware and spam controls must be implemented and continuously updated to protect all Air Force information technology in accordance with DoD Instruction 8500.01 and Air Force Manual 17-1301 **(T-0)**; organizations owning or operating devices that connect to systems that are not capable of integrating/supporting anti-malware protections must ensure that these devices are provisioned with malware protections that are regularly updated. **(T-1)**.

4.4.2.8. Software and firmware patches must be applied in accordance with Air Force Space Command and 24th Air Force guidance. **(T-1)**.

4.4.2.9. External Service Providers' and Trading Partners' authorized connections to Air Force networks will be subject to the same continuous monitoring rigor as that applied to Air Force systems. **(T-1)**.

4.4.3. **Detection Processes.** Risk will be subjected to continuous monitoring at all command levels. In accordance with DoD Instruction 8510.01 and Air Force Instruction 17-101, Information System Owners /System Managers and/or Program Managers must develop a formal continuous monitoring strategy with an implementation plan and procedures for their respective systems. **(T-0)**. Strategy documents must describe:

4.4.3.1. The assignment of responsibility and delegation of authority for strategy execution. **(T-1)**.

4.4.3.2. The approach for a continual monitoring and assessment of the system's security posture. See Attachment 13, Cyber Mission Readiness. **(T-1)**.

4.4.3.3. The design of all security controls within or inherited by the system, and an assessment of their expected effectiveness. **(T-1)**.

4.4.3.4. The plan and schedule for regular scans. The strategy must detail required rules of engagement for scanning evolutions, what is expected to be scanned and how often, as well as how scan results will be aggregated and reported. See Attachment 13. **(T-1)**.

4.4.3.5. Key internal and external stakeholders, and the procedures for exchanging relevant information with them. **(T-1)**.

4.4.3.6. Requirements for remaining cognizant of, and reacting in a timely manner to, all alerts and advisories from United States Cyber Command and 24th Air Force. **(T-0)**.

4.4.3.7. Continuous monitoring plans and processes must be integrated with the System Security Plan, and approved by the cognizant Authorizing Official. **(T-1)**.

4.5. Respond

The Air Force Cybersecurity Program addresses the Framework's Respond function by providing for the ability to effectively and appropriately respond to undesirable events and incidents in accordance with guidance contained in DoD Instruction 8530.01, and the Air Force issuances cited below **(T-0)**:

4.5.1. **Response Planning**. A formal incident response plan with guidance and procedures compliant with the requirements articulated in Air Force Instruction 10-1701, *Command and Control (C2) for Cyberspace Operations*, and Air Force Manual 17-1301, must be developed for each system or enclave **(T-1)** that describes:

4.5.1.1. Incident standards and criteria to help determine the point at which a reportable event is formally declared an incident, triggering the activation of the incident response plan. **(T-2)**.

4.5.1.2. Detailed implementation procedures to be executed when an incident is declared. **(T-2)**.

4.5.1.3. The incident response chain of command **(T-1)**, including the identification of the persons/offices that are empowered to:

4.5.1.3.1. Declare and downgrade a formal incident, to declare an incident. closed/resolved, and to escalate a formal incident to a continuity or disaster event.

4.5.1.3.2. Manage the incident, to include the marshalling and direction of response resources.

4.5.1.3.3. Implement incident response procedures; the plan should establish the minimum required qualifications and skill sets per the standards articulated in Department of Defense 8570.01-M and Air Force Manual 17-1303. **(T-0).**

4.5.1.4. The schedule for training incident response resources **(T-1)** to ensure that incident response team members are aware of their roles and responsibilities when responding to an incident.

4.5.2. **Communications.** Incident response plans must identify key internal and external stakeholders, and describe the procedures and modalities for exchanging relevant information with them, to include information that is shared to achieve broader Air Force-wide situational awareness. See Air Force Instruction 10-1701 for details concerning the Air Force network response hierarchy. **(T-1)**.

4.5.3. **Analysis.**

4.5.3.1. Incident response plans and procedures must be executed on a proactive basis; systems must be configured to alert or provide timely notification of anomalous behaviors; cybersecurity personnel must actively and continuously seek out evidence of potentially undesirable events. **(T-2)**.

4.5.3.2. Incident response plans and procedures should forecast expected impacts from various incident scenarios. **(T-2)**.

4.5.3.3. All incidents must be subjected to post-event analysis, categorization, and forensics in accordance with the incident response plan. **(T-2)**. The sensitivity of the analysis must be evaluated in light of the risk to mission operation and national security interests, and classified if necessary in accordance with the terms of Executive Order 12958, as amended. **(T-0)**. Air Force organizations that are not sufficiently resourced with the skill sets required to conduct such investigations will request support from 24th Air Force.

4.5.4. **Mitigation.** Flaws discovered during incidents must be remediated **(T-1)**, ensuring that:

4.5.4.1. The proximate cause of the incident is contained. **(T-3)**.

4.5.4.2. Newly discovered vulnerabilities are mitigated or documented as risks that have been formally accepted by the cognizant Authorizing Official. **(T-2)**.

4.5.4.3. Software and firmware updates related to flaw remediation are tested for effectiveness and potential side effects before installation. **(T-3)**.

4.5.4.4. Security-relevant software and firmware updates are installed within their mandated time periods. **(T-2)**.

4.5.4.5. Flaw remediation is integrated into the configuration management process; DoD Instruction 8510.01 and Air Force Instruction 17-101 are germane. **(T-1)**.

4.6. Recover

The Air Force Cybersecurity Program provides for the ability to recover from incidents and events that impact mission operations in accordance with guidance contained in Air Force Instruction 10-208, *Air Force Continuity of Operations (COOP) Program*. **(T-1)**.

4.6.1. **Recovery Plans.** Strategies, plans, processes and standards for recovering from cybersecurity incidents and continuity events must be developed, approved, promulgated and regularly tested, as described in the sections below. **(T-1).**

4.6.1.1. Formal information technology contingency plans specific to each Air Force system or enclave must be developed **(T-1)** to:

4.6.1.2. Define essential missions and functions, **(T-1)**.

4.6.1.3. Establish recovery objectives for relevant systems, **(T-2)**.

4.6.1.4. Describe authorities and their roles and responsibilities. Ensure that the person or persons who is/are delegated the authority to declare and terminate a continuity event are clearly identified, **(T-3)**.

4.6.1.5. Establish measures to maintain critical functions **(T-3)**, and

4.6.1.6. Establish full restoration procedures. **(T-3)**.

4.6.2. **Communications.** Define a public relations strategy, including measures that could be taken to repair a damaged Command/Air Force reputation. Ensure that recovery activity status is communicated clearly and regularly to external stakeholders, and to leadership and management teams in the organizational chain of command. **(T-2)**.

4.6.3. **Service Level Agreements and Memorandums of Agreement/Understanding.** Organizations that may temporarily assume responsibility for executing critical mission/system functions, and execute formal agreements to specify each organizations' responsibilities and service level commitment must be identified, and agreed-upon service levels are described. **(T-2)**.

4.6.4. **Plan testing.** Recovery plans must be formally tested no less than annually, with test results and lessons learned documented and retained. **(T-2)**.

4.6.5. **Improvements.** Recovery strategies plans and procedures are informed and modified to incorporate lessons learned from exercise evolutions and actual recovery events. **(T-2)**.

Attachment 1 – GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Air Force Instruction 33-200_AFGM2016-01, *Air Force Cybersecurity Program Management*, 18 October 2016 (hereby cancelled)

Air Force Instruction 33-360, *Publications and Forms Management*, 30 November 2016

Air Force Manual 33-363, *Management of Records*, 02 June 2017

Air Force Policy Directive 17-1, *Information Dominance Governance and Management*, 12 April 2016

Air Force Policy Directive 33-2, *Information Assurance Program* (superseded)

Air Force Instruction 33-200, *Information Assurance (IA) Managemen*t (superseded)

Air Force Mission Directive 1-26, *Chief, Information Dominance and Chief Information Officer,* 05 February 2015

National Institute for Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, 10 January 2017

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 11 May 2017

44 United States Code 3554, *Federal agency responsibilities*

Department of Defense Instruction 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*, 08 June 2008

National Security Presidential Directive/Homeland Security Presidential Directive-54/-23, *Cybersecurity Policy*, 08 January 2008

National Institute for Standards and Technology Special Publication 800-39, *Managing Information Security Risk*, March 2011

Department of Defense Instruction 8510.01, Change 1, *Risk Management Framework (Risk Management Framework) for Department of Defense Information Technology (IT)*, 24 May 2016

Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, 06 April 2015

10 United States Code 2224, *Defense Information Assurance Program*

Department of Defense Instruction 8500.01, *Cybersecurity*, 14 March 2014

Air Force Instruction 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, 02 February 2017

Department of Defense Instruction 5000.02, Change 2, *Operation of the Defense Acquisition System*, 02 February 2017

Air Force Manual 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, 09 May 2017

Air Force Manual 17-1203, Change 2, *Information Technology (IT) Asset Management (Information Technology Asset Management)*, 07 March 2017

Public Law 113-283, (44 United States Code § 3551, et seq.), *Federal Information Security Modernization Act of 2014 (FISMA)*

Air Force Operational Test and Evaluation Center Manual 99-101, *Operational Test Processes and Procedures*, 11 October 2012

Air Force Operational Test and Evaluation Center Pamphlet 99-104, *AFOTEC Operational Suitability Test and Evaluation Guide*, 01 May 2007

Department of Defense Identity and Access Management (IdAM) Strategy, Version 1.0, October 17, 2014.

44 United States Code 3545, *Annual independent evaluation*

Department of Defense Instruction 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA)*, 29 January 2010

Department of Defense Instruction 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, 09 July 2004

Air Force Manual 17-1303, *Cybersecurity Workforce Improvement Program*, 01 November 2016

Air Force Manual 17-1302-O, *Communications Security (COMSEC)* Operations, 03 February 2017

Air Force System Security Instruction 7702, Change 1, *Emission Security Countermeasures Reviews*, 17 October 2008

Department of Defense Directive 8140.01, *Cyberspace Workforce Management*, 11 August 2015

Department of Defense 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005

Air Force Instruction 10-206, *Operational Reporting*, 05 June 2017

Department of Defense Instruction 8551.01, *Ports, Protocols, and Services Management (PPSM)*, 28 May 2014

Air Force Instruction 90-201, *The Air Force Inspection System*, 26 January 2017

Air Force Instruction 10-712, *Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process*, 17 December 2015

Air Force Manual 17-1301, *Computer Security (COMPUSEC)*, 10 February 2017

Air Force Instruction 71-101, Volume 3, *The Air Force Technical Surveillance Countermeasures Program*, 13 May 2015

Air Force Instruction 17-203, *Cyber Incident Handling*, 16 March 2017

Commander, Joint Chiefs of Staff Manual 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

Department of Defense Instruction 8530.01, *Cybersecurity Activities Support to Department of Defense Information Network Operations*, 07 March 2016

Air Force Instruction 63-101/20-101, *Integrated Life Cycle Management*, 09 May 2017

Undersecretary of Defense - Acquisition, Training and Logistics MIL-HDBK-61A(SE), *Configuration Management*, 07 February 2001

Air Force Instruction 17-110, *Air Force Information Technology Portfolio Management and Investment Review*, 28 October 20016

Office of Management and Budget Circular A-130, *Management of Information as a Strategic Resource*, 28 July 2016

Methods and Processes Technical Order 00-33B-5006, *End Point Security for Information Systems*, 19 December 2012

Air Force Manual 17-1202, *Collaboration Services and Voice Systems Management*, 04 November 2014

Committee on National Security Systems Instruction 5006, *National Instruction for Approved Telephone Equipment*, September 2011

Department of Defense Instruction 8115.02, *Information Technology Portfolio Management Implementation*, 30 October 2006

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, 12 February 2013

Department of Defense Directive 8000.01, *Management of the Department of Defense Information Enterprise (Department of Defense IE)*, 17 March 2016

Air Force Instruction 10-701, *Operations Security (OPSEC)*, 28 July 2017

Chairman, Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, 09 February 2011

Chairman, Joint Chiefs of Staff Instruction 6211.02D, *Defense Information Systems Network (DISN) Responsibilities*, 24 January 2012

Air Force Instruction 10-712, *Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process*, 17 December 2015

Department of Defense Directive 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (Department of Defense) Global Information Grid (GIG)*, 14 April 2004

Department of Defense Directive 8521.01E, *Department of Defense Biometrics*, 13 January 2016

Department of Defense 5200.08-R, Change 1, *Physical Security Program*, 27 May 2009

Department of Defense-M 5205.07V3_Air Force Manual16-703V3, *Department of Defense Special Access Program (SAP) Security Manual: Physical Security*, 03 November 2008

United States Cyber Command CTO 08-001, *Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media Used Within the Department Of Defense (Department of Defense),* 08 January 2008

5 United States Code 552a, *The Privacy Act of 1974*

Federal Information Processing Standard 140-2, Change Notice 2, *Security Requirements for Cryptographic Modules,* 03 December 2002

Executive Order 13526, as amended, *Classified National Security Information,* 29 December 2009

Executive Order 13556, as amended, *Controlled Unclassified Information,* 28 March 2003

Department of Defense Manual 5200.01, Volume 2, Change 2, *Department of Defense Information Security Program: Marking of Classified Information,* 19 March 2013

Department of Defense Manual 5200.01, Volume 4, *Department of Defense Information Security Program: Controlled Unclassified Information (CUI),* 24 February 2012

Department of Defense 5400.11-R, *Department Of Defense Privacy Program,* 14 May2007

Department of Defense Directive 5400.11, *Department of Defense Privacy Program*, 29 October 2014

Air Force Instruction 33-332, Change 1, *The Air Force Privacy and Civil Liberties Program,* 17 November 2016

Department of Defense Instruction 5015.02, *Department of Defense Records Management Program*

Department of Defense Instruction 5015.02, *Department of Defense Records Management Program*, 24 February 2015

Department of Defense 5220.22-M, Change 2, *National Industrial Security Operations Manual (NISPOM),* 18 May 2016

Department of Defense Instruction 5200.44, Change 1, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),* 25 August 2016

Air Force Pamphlet 63-113, *Program Protection Planning for Life Cycle Management*, 17 October 2013

Air Force Instruction 17-140, *Air Force Architecting*, 20 October 2016

Committee on National Security Systems Policy 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products,* 10 June 2013

Department of Defense Instruction 5134.16, *Deputy Assistant Secretary of Defense for Systems Engineering (DASD (SE)),* 19 August 2011

Air Force System Security Instruction 8551, *Ports, Protocols, and Services Management (PPSM)*

Department of Defense Instruction 4000.19, *Support Agreements,* 25 April 2013

Department of Defense Instruction 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, 24 May 2011

Department of Defense Instruction 8520.03, *Identity Authentication for Information Systems*, 13 May 2011

Air Force Manual 17-1302-O, *Communications Security (COMSEC) Operations*, 03 Feb 2017

Department of Defense Instruction 8540.01, *Cross Domain (CD) Policy*, 05 August 2015

Air Force System Security Instruction 7702, *Emission Security Countermeasures Reviews, Change 1*, 17 October 2008

Air Force Manual 17-2101, *Long Haul Communications Management*, 20 October 2016

Air Force Policy Directive 51-2, *Administration of Military Justice*, 04 November 2011

Air Force Instruction 10-1701, *Command and Control (C2) for Cyberspace Operations*, 12 May 2016

Air Force Instruction 10-208, *Air Force Continuity of Operations (COOP) Program*, 15 December 2011

Prescribed Forms

Form DD2875, *System Access Authorization Request*

Air Force Form 4170, *Emission Security Assessments/Emission Security Countermeasures Reviews*

Air Force Form 4169, *Request for Waiver from Information Assurance Criteria*

Attachment 2 – Air Force Information Technology User Responsibilities

A2.1. Overview:

A2.1.1. Protecting the confidentiality, integrity, and availability of information that is processed, stored or transmitted through the system may require a great number of discrete controls, and while privileged users may be required to maintain a finer-grained understanding of their control obligations, Air Force Information Technology users are not expected to be familiar with the details of every control.

A2.1.2. All Air Force Information Technology users will instead be required be familiar with and comply with a short list of dos and don'ts that more closely pertain to their everyday experience with Air Force Information Technology.

A2.2. Implementation:

A2.2.1. All Air Force Information Technology Users must observe the requirements in DoD Regulation 5500.7-R, *Joint Ethics Regulation (JER)* **(T-0)**, and comply with the guidance contained in Air Force Instruction 10-701, *Operations Security*, Air Force Instruction 33-322, *Records Management*, Air Force Instruction 33-364, *Records Disposition-Procedures and Responsibilities*, Air Force Instruction 33-332, *Privacy Act Program*, Air Force Manual 33-363, *Management of Records*, and comply with public affairs Internet-based capabilities guidance and related issuances. **(T-0)**.

A2.2.2. To this end, all Air Force Information Technology users must read and sign Rules of Behavior agreements prior to be granted access to Air Force Information Technology. **(T-1)**; see Annex 1 to this Attachment. Rules of Behavior agreements should:

A2.2.2.1. Be instantiated as a list.

A2.2.2.2. Articulate in short declarative sentences what is explicitly allowed and what is explicitly proscribed.

A2.2.2.3. Address rules that every users must read, internalize, and apply in their normal, day-to-day jobs.

A2.2.3. Rules of Behavior should be designed to reinforce the concept that every authorized Air Force Information Technology user accepts responsibility for protecting the system from compromise, commensurate with privileges associated with their role. Rules of Behavior agreements must require that, as a condition of employment and/or access, Air Force Information Technology users:

A2.2.3.1. DO adhere to legal, regulatory **(T-0)**, and command **(T-0)** requirements.

A2.2.3.2. DO use Air Force Information Technology in a manner that protects and preserves information confidentiality, integrity and/or availability. **(T-2)**.

A2.2.3.3. DO use Air Force Information Technology in a manner that protects and preserves the physical integrity of Air Force Information Technology and Air Force cyberspace assets and resources. **(T-3)**.

A2.2.3.4. DO NOT attempt to exceed the limits of authorized access and privilege. **(T-2)**.

A2.2.3.5. DO NOT use Air Force Information Technology in a manner which may tend to bring discredit on users or the Air Force, or degrade the Air Force's ability to execute on its assigned missions, except for disclosure protected by Whistleblower statues. **(T-1)**.

A2.2.3.6. DO NOT waste Air Force Information Technology or Air Force cyberspace assets and resources. **(T-2)**.

A2.2.3.7. DO NOT connect Air Force Information Technology through public networks (Internet cafés and kiosks, hotel business centers, home networks, etc.) for processing government-owned information unless mobile computing device encryption and connection policies are followed. **(T-3)**.

A2.2.4. Disciplinary Actions

A2.2.4.1. **Failure to observe the prohibitions and mandatory provisions of this Attachment by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ),* Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action in accordance with AFI 36-703, *Civilian Conduct and Responsibility,* without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel may be handled according to applicable laws and the terms of the contract. Additionally violations of this Attachment by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. (T-0).**

Annex 1 - Rules of Behavior and Acceptable Use Standards for Air Force Information Technology

The following statements reflect mandatory behavioral norms and standards of acceptable use of Air Force Information Technology. By signing below, you indicate both your understanding of these standards, and your agreement to act in accordance with them as a condition of your service with or access within the Air Force. Air Force Instruction 17-130, *Cybersecurity Program Management*, applies.

1. I WILL adhere to and actively support all legal, regulatory, and command requirements.

a. I understand that Air Force Information Technology is to be used primarily for Official/ Government Business, and that limited personal use must be of reasonable duration and frequency that have been approved by the supervisors and do not adversely affect performance of official duties, overburden systems or reflect adversely on the Air Force or the DoD.
b. I will not use my access to government information or resources for private gain.
c. I waive my expectation of privacy in my Air Force electronic communications. This is not a waiver of my rights to attorney-client privilege, medical information privacy, or the privacy afforded communications with religious officials/chaplains.
d. I will observe all software license agreements and Federal copyright laws.
e. I will encrypt sign and any message containing For Official Use Only or Personally Identifiable Information.
f. I will promptly report all security incidents in accordance with Air Force policy.

2. I WILL use the system in a manner that protects information confidentiality, integrity and/or availability.

a. I will not store or process classified information on any system not approved for classified processing.
b. I will protect my Common Access Card token from loss, compromise, or premature destruction. I will not share my token/credentials with anyone, use another person's token/credentials, or use a computer or terminal on behalf of another person.
c. I will protect my passwords/Personal Identification Numbers from disclosure: I will not post or write these down in my work space.
d. I will lock or log-off my computer or terminal any time I walk away.
e. I understand that my password/Personal Identification Numbers must adhere to current Air Force standards for length, key-space, and aging requirements.
f. I will not disclose any non-public Air Force or DoD information to unauthorized individuals.
g. I understand that everything done using my Common Access Card/password/Personal Identification Number will be regarded as having been done by me.
h. I will employ anti-malware software and update it as required; I will immediately notify my Information System Security Officer if I believe Air Force Information Technology assets entrusted to me have been compromised; I will take immediate measures to limit damage.

3. I WILL protect the physical integrity of computing resources entrusted to my custody or use.

a. I will protect Air Force Information Technology from hazards such as liquids, food, smoke, staples, paper clips, etc.
b. I will protect Air Force Information Technology from tampering, theft or loss; I will take particular care to protect any portable devices and media entrusted to me, such as laptops, cell phones, tablets, disks, and other portable electronic storage media.
c. I will protect Air Force Information Technology storage media from exposure to physical, electrical, and environmental hazards. I will ensure that media is secured when not in use based on the sensitivity of the information contained, and practice proper labeling procedures.
d. I will not allow anyone to enter DoD or Air Force facilities without proper authorization.
e. I will not install, relocate, modify, or remove any Air Force Information Technology without proper approval.

4. I WILL NOT attempt to exceed my authorized privileges.

a. I will not access, research, or change any account, file, record, or application not required to perform my job.
b. I will not modify the operating system configuration on Air Force Information Technology without proper approval.
c. I will not move equipment, add or exchange system components without authorization by the appropriate approval of my local systems manager or local hardware custodial personnel.
d. I will not use, or connect to, non-official hardware, software or networks for official business without proper approval and without the use of authorized mobile device network encryption.

5. I WILL NOT use systems in a way that brings discredit on Air Force users or the Air Force, or degrade Air Force missions.

a. I will practice operational security in accordance with guidance contained in Air Force Instruction 10-701, *Operations Security*.
b. I will not receive or send inappropriate material using my official email or Internet accounts.
c. I will not originate or forward chain letters, hoaxes, or items that advocate or support a political, moral or philosophical agenda.
d. I understand that pornography, sexually explicit or sexually oriented material, nudity, hate speech or ridicule of others on the bases of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin), gambling, illegal weapons, militant, extremist, or terrorist activities will not be tolerated.
e. I will not connect or remove any form of removable media without proper approval.

6. I WILL NOT waste system and network resources.

a. I will not make excessive use of my official computer to engage with social media for personal purposes (e.g., Facebook, Twitter, Instagram, Snapchat, etc.)
b. I will not make excessive use of my official computer for shopping, or to view full-motion video from non-official sources (e.g., YouTube, online multiplayer video games, etc.)
c. I will not autoforward e-mail from my official account to a personal e-mail account.

_____ _____

Signature Date

_____ _____

Printed name (Last, First, MI) Rank/Position

Attachment 3 – Reserved

Attachment 4 – Access Control

A4.1. Overview: Access controls limit or detect improper access to Air Force Information Technology resources (i.e., information, hardware, software, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls. Logical access controls require users to authenticate themselves in order to access Air Force Information Technology resources and limit the files and other resources that they can access, and limit the actions that they can execute. Physical access controls involve mediating physical access to Air Force Information Technology resources and protecting them from intentional or unintentional loss or impairment. Without adequate access controls, unauthorized internal and/or external individuals can intentionally read and copy sensitive data, make undetected changes or deletions for malicious purposes or personal gain, intentionally or unintentionally read, add, delete, modify, or exfiltrate data or execute changes that are outside their span of authority, introduce errors that impact mission execution, or cause physical damage to Air Force Information Technology resources.

A4.2. Implementation.

A4.2.1. Physical and logical access to all Air Force Information Technology must be mediated using the most reliable and secure technology available, consistent with risk, Air Force standards, and operational requirements. **(T-1).**

A4.2.2. Air Force Information Technology information systems, as defined in the introduction to this Instruction, must:

A4.2.2.1. Enforce information flows:

A4.2.2.1.1. Air Force Information Technology must adhere to a Discretionary Access Control architecture, supported by a Role Based Access Control model when technically feasible. **(T-2).**

A4.2.2.1.2. Information at a lower level of sensitivity or classification may be written up to a container holding information at a higher level of sensitivity or classification. **(T-3)**. Information at a higher level of sensitivity or classification must not be written down to a container holding information at a lower level of sensitivity or classification, except through a controlled interface such as Defense Information System Agency-approved High Assurance Guard, or when the system or systems is/are accredited and authorized to operate in a multilevel mode. **(T-0).**

A4.2.2.2. Be configured to limit unsuccessful access attempts by locking the Air Force Information Technology asset after a no less than three number of attempts until released by an administrator. **(T-1).** Waivers and modifications to this standard may be granted by the cognizant Authorizing Official via record correspondence.

A4.2.2.3. Display the Air Force-wide standard acceptable use banner upon login that requires user acknowledgment before granting access to Air Force Information Technology resources. **(T-1).**

A4.2.2.4. Conspicuously display an on-screen classification banner that is continuously visible while the system is logged into. Systems that do not feature a user screen or monitor must be physically tagged to indicate the highest level of classification that the device can process, transmit, display or store. **(T-1).**

A4.2.2.5. Be configured to initiate a session lock in accordance with applicable Security Technical Implementation Guides/Security Requirements Guides, or after 10 minutes of inactivity, whichever is more restrictive, and terminate the session in accordance with applicable Security Technical Implementation Guides/Security Requirements Guides, or after 2 hours of inactivity, whichever is more restrictive. **(T-1).** Units may instantiate stricter standards at their discretion, consistent with risk and mission needs. **(T-3).** Waivers to relax these standards may be granted by the cognizant Authorizing Official via record correspondence.

A4.2.3. Remote access to the Air Force Information Network for telework and remote administration is permitted, with the following conditions and restrictions:

A4.2.3.1. Criteria for determining eligibility for telework are identified in DoD Instruction 1035.01, *Telework Policy*, and Air Force Instruction 36-816, *Civilian Telework Program*. User's remote access must be approved in advance by cognizant management, employing the DD Form 2946, *DoD Telework Agreement*. **(T-0).**

A4.2.3.2. Remote access and processing is allowed only at the UNCLASSIFIED level unless explicitly authorized by the cognizant command and cognizant Authorizing Official. **(T-1).**

A4.2.3.2.1. If classified telework is authorized at an approved alternative secure location, users must comply with procedures established by Air Force regarding such work. **(T-1).** Refer to Air Force Instruction 16-1404, *Information Security Program Management*, for guidance on Information Protection.

A4.2.3.2.2. Remote privileged access (e.g., for remote administration) must be justified, with the rationale for allowing such access documented in detail in the remote access agreement. **(T-3)**. Curt, non-descriptive rationales such as "needed for work" or "system administrator" are not acceptable. **(T-1).**

A4.2.3.3. All remote access connections must be effected through a managed access point, and must be protected using Air Force-authorized Virtual Private Network technology, In accordance with *Defense Information System Agency Remote Access Policy, Remote Endpoint, and Remote Access VPN* Security Technical Implementation Guides. **(T-0)**.

A4.2.3.4. Remote access to the Air Force Information Network is allowed from external systems, e.g., systems owned, administered, maintained and operated by

organizations external to Air Force, to include other DoD, federal state, local, tribal, non-governmental and contractor organizations. **(T-3).** The guidance in this section does not apply to the use of external information systems to access public interfaces to Air Force Information Technology; otherwise, the following conditions and restrictions apply:

A4.2.3.4.1. Third-parties' systems access must be governed through a formal third-party agreement between Air Force and the owner of the external system, e.g. law, policy, contract, Memorandums of Agreement or Understanding. Air Force and its third-party partners will each retain a copy of the agreement. **(T-1)**. DoD Instruction 4000.19, *Third Party Agreements*, is germane.

A4.2.3.4.2. Third party agreements must explicitly specify the terms and conditions under which an external system may be allowed to access Air Force Information Technology resources. **(T-1)**. Terms and conditions may be more restrictive, but cannot be less restrictive, than the terms of this Instruction. **(T-1)**. In cases where less restrictive controls are necessitated by business/mission requirements, third party access must be confined to a Demilitarized Zone. **(T-1)**.

A4.2.3.4.3. In cases where responsibility for security control implementation, maintenance, and monitoring are shared between Air Force and a third party, the division of responsibilities must be explicitly addressed in the third party agreement. **(T-1)**.

A4.2.3.4.4. Compliance with the terms of third-party agreements must be included in the Risk Management Framework authorization package, and included in the continuous monitoring regime. **(T-1)**.

A4.2.3.5. Remote access requires two-factor authentication; the requirement for two-factor authentication is mandatory, with no waivers allowed. **(T-0)**.

Attachment 5 – Account Management

A5.1. Overview: Account management encompasses standards and processes to govern how potential users gain access to Air Force Information Technology resources, how their access authorizations and privileges are established and tracked, and how the user account life cycle is managed over time, from initial account establishment, through account modification due to promotion, demotion, job change, retirement or departure. Air Force Information Technology accounts must be carefully administered to satisfy mission requirements on an uninterrupted basis, while ensuring that duties are properly segregated and privileges managed to prevent one person from gaining excessive control over an entire mission/business process.

A5.2. Implementation:

A5.2.1. All Air Force Information Technology will identify and maintain user accounts to control access and maintain personal accountability. **(T-1)**.

A5.2.2. All organizations owning or operating Air Force Information Technology will:

A5.2.2.1. Ensure that account management guidance and processes are properly reflected in system security plans. **(T-1)**.

A5.2.2.2. Identify and define account types[1] (e.g., non-privileged, privileged, guest, maintenance) to support organizational missions/business functions for Air Force Information Technology under their cognizance. **(T-1)**.

A5.2.2.3. Actively manage Air Force Information Technology accounts; for each account type, authorized users must be specified, group and role membership conditions/requirements defined, and access authorizations/privileges and other attributes (as required) assigned. **(T-1)**. Attachment 4, *Access Control* and Attachment 6, *Identification and Authentication*, are germane.

A5.2.2.4. Develop procedures for managing the user account life cycle; procedures must define the circumstances and actions to be taken to create, enable, modify, suspend, disable and remove/retire user accounts. **(T-3)**.

A5.2.2.5. Develop procedures to annually revalidate, and as necessary, modify privileged and non-privileged accounts.

A5.2.3. Formal approvals are required for account establishment using the DD Form 2875; each users' workplace supervisor must specify and justify the privileges to be granted, and the cognizant Information Owner, Information System Security Officer, and Information System Security Manager must approve. **(T-1)**. See also Attachment 7, *Segregation of Duties and Least Privilege* for details on privilege management.

A5.2.3.1. Electronic DD 2875s and associated documents are preferred over hard copy, digital signatures are preferred over wet signatures.

[1] Account types will vary widely by system, and should reflect and support each systems' mission.

A5.2.3.2. Section A4.2.15 describes alternative requirements for organizations with high PERSTEMPO, e.g. schoolhouses and training commands.

A5.2.4. Access and privilege authorizations must be based on:

A5.2.4.1. A valid need-to-access/need-to-know; users requiring elevated/administrative/ cybersecurity privileges on information system accounts will receive additional scrutiny by account approval authorities. **(T-0)**.

A5.2.4.2. Intended system usage. **(T-3)**.

A5.2.4.3. Other attributes as required by missions/business functions. **(T-3)**.

A5.2.5. Foreign Nationals. Non-U.S. citizens/permanent residents may be provisioned with accounts granting access to Air Force Information Technology and associated networks and resources in accordance with the requirements of this Attachment, in addition to the following requirements and conditions:

A5.2.5.1. The subject Foreign National must be covered by a valid host-nation agreement. **(T-0).**

A5.2.5.2. Foreign National clearance and need-to-know must be validated prior to account establishment. **(T-0)**. In accordance with DoD 5200.02-R, *Personnel Security Program*, only U.S. citizens are eligible for a security clearance; however, compelling reasons may exist to grant access to classified information to an immigrant alien or a foreign national using a "Limited Access Authorization". **(T-2)**. DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, and DoD Directive 5230.20, *Visits and Assignments of Foreign Nationals*, are also germane.

A5.2.5.3. Foreign National access to Air Force Information Technology must be addressed in accessed systems' Risk Managed Framework assessment package(s). **(T-1)**.

A5.2.6. Modification of existing accounts must take into account the principles of least privilege and segregation of duties. **(T-1)**; see Attachment 7. Modification procedures must be designed to guard against 'privilege creep', i.e., allowing users to acquire more and more privileges to gain excessive control over a mission/business process. **(T-1)**.

A5.2.7. Accounts must be suspended or disabled when:

A5.2.7.1. A user is assigned to temporary duty and cannot be expected to employ their authorized account for a period of 45 or more days. **(T-3)**.

A5.2.7.2. An account is idle for 45 or more days; idle account suspensions must be automated. **(T-3)**.

A5.2.7.3. An authorized user transfers or retires. **(T-1)**.

A5.2.7.4. A user is suspected of conduct that could result in their reassignment, removal, or dismissal. **(T-2)**. In such cases, the account can be reactivated upon cognizant management approval.

A5.2.8. Accounts must be removed/retired no more than:

A5.2.8.1. Thirty (30) days after an authorized user transfers or retires. Key files and logs must be saved or transferred prior to account removal. **(T-3)**.

A5.2.8.2. Ten (10) days after a user is moved into a different group/role or their need-to-know changes. Key files and must be saved or transferred prior to account removal. **(T-3)**.

A5.2.9. Account management procedures must address the use of temporary accounts as a part of normal account activation, when there is a need for short-term accounts without the demand for immediacy in account activation. **(T-1)**. Temporary accounts must be suspended when no longer needed, but are not subject to automatic suspension/deletion. **(T-3)**.

A5.2.10. Account management procedures must address account creation and suspension/deletion for deployed organizations and Air Force Information Technology; a process for reissuing shared/group account credentials when individuals are removed from the group must be designed and implemented. **(T-1)**.

A5.2.11. Account management procedures must address account creation and suspension/deletion in emergency circumstances, as described below:

A5.2.11.1. Emergency accounts will be created only under circumstances that could otherwise result in substantial mission degradation or mission failure; they must not be used for administrative convenience. **(T-1)**.

A5.2.11.2. Emergency account establishment procedures may bypass normal account authorization processes, however, a chain of accountability must be maintained. **(T-1)**.

A5.2.11.3. Emergency account justifications must detail the potential impacts resulting from failure to establish such accounts. **(T-1)**.

A5.2.11.4. Emergency accounts must be assigned to individuals; group emergency accounts are proscribed. **(T-1)**.

A5.2.11.5. All actions performed through emergency accounts must be logged, and logs examined by cognizant personnel. **(T-1)**.

A5.2.11.6. Emergency accounts must be suspended and/or deleted within an organizationally defined time period, but are not subject to automatic suspension/deletion. **(T-3)**. Key files and logs must be saved or transferred to another user prior to account removal. **(T-2)**.

A5.2.12. Account management procedures must address account creation and suspension/deletion in exigent circumstances, as described below:

A5.2.12.1. Accounts terminated under hostile/adverse circumstances must be designed to limit/prevent any harmful measure that may be taken by the terminated user, and to ensure the availability and integrity of suspended users files and audit trails for business continuity and/or damage assessment purposes **(T-1)**; a minimum of 90 previous calendar days' worth relevant files and audit trails must be preserved and transferred to cybersecurity personnel and/or law enforcement. **(T-3)**.

A5.2.13. All Air Force Information Technology capable of doing so will automatically audit for and notify account managers of account creation, modification, enabling, disabling, and removal actions. **(T-3)**.

A5.2.14. Systems that feature automated mechanisms to support the management of information system accounts are preferred.

A5.2.15. Air Force organizations that experience a high PERSTEMPO by virtue of their mission (schoolhouses, training commands, etc.) may employ the following techniques to ease the administrative burden of managing DD Form 2875s, as described in the following sections:

A5.2.15.1. Create an attachment that contains the names of all Temporary Duty/ Temporary Additional Duty population members and the role(s)/privileges they are authorized. If different members among the population will be granted access to different roles/privileges, indicate the relevant role(s)/privileges next to each name.

A5.2.15.1.1. In circumstances where Temporary Duty/Temporary Additional Duty personnel arrive aperiodically rather than simultaneously in a class/cadre structure, create an attachment that is revised every 1-6 months, depending on PERTEMPO.

A5.2.15.2. Have the individual in the Supervisor role sign and provide a date-time group the attachment document.

A5.2.15.3. For each system and temporary user population, create and process a single DD Form 2875 that is signed by all required authorities.

A5.2.15.4. In Block 13, enter the justification for the entire population requiring access. The justification description may be brief, but not perfunctory; entries such as “Students” or “Needed for course” are not acceptable.

A5.2.15.5. Enter the Supervisor name and Attachment date-time group into Block 13; attach the relevant Attachment to the DD 2875 and file.

A5.2.15.6. After the temporary users have completed their class/training, delete their access and so note it on the DD 2875.

A5.2.15.7. Retain the DD 2875 and attachment for a minimum of one year.

Attachment 6 – Identification and Authentication (I&A)

A6.1. Overview: Identification and authentication of subjects accessing Air Force Information Technology is a key cybersecurity control. *Identification* refers to the proofing to establish that a subject is who or what they claim to be. Digital *authentication* establishes that a subject attempting to access a cyber resource is in control of one or more valid authenticators associated with that subject's digital identity. Digital authentication presents a technical challenge because this process often involves the authentication of individual subjects over an open network to access Air Force Information Technology devices and services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks. For this reason, Air Force Information Technology and information owners need a level of confidence that the digital identity accessing their cyber resources is the legitimate proxy to the real-life, authorized subject.

A6.2. Implementation. In accordance with Section 4.3.1 of this Instruction:

A6.2.1. All Air Force Information Technology must be capable of uniquely identifying and authenticating authorized users or processes acting on behalf of authorized users. **(T-0)**.

A6.2.1.1. Two-factor authentication must be implemented on all Air Force Information Technology capable of supporting the function **(T-3)**; two-factor authentication using the DoD Common Access Card is the primary mechanism. Alternative two-factor authentication mechanisms that feature acceptance and electronic verification of Personal Identity Verification credentials are allowed on a case-by-case basis by the cognizant Authorizing Official. **(T-1)**.

A6.2.1.1.1. Two-factor authentication is required for network and local access to privileged accounts, and for network access to non-privileged accounts. **(T-0)**. Two-factor authentication is required for remote access to privileged and non-privileged accounts.

A6.2.1.1.2. Air Force Information Technology capable of supporting the function will implement replay-resistant authentication mechanisms for network access to privileged accounts.

A6.2.2. All network-connected Air Force Information Technology devices must uniquely identify and authenticate before establishing a network or remoted connection to the Air Force Information Network **(T-1)**; Technical Order 00-33A-1106, *Air Force Information Network (AFIN) Network Management*, guidance on implementing and configuring IEEE 802.1x services is germane. Additionally, In accordance with DoD Instruction 8500.01, *Cybersecurity*, all Air Force Information Technology will be configured to include a Trusted Platform Module version 1.2 or higher where required by Defense Information Systems Agency Security Technical Implementation Guides and where technically feasible. **(T-0)**.

A6.2.2.1. Vendor Trusted Platform Modules must be in conformance with Trusted Computing Group standards (www.trustedcomputinggroup.org/groups/tpm) and must be

approved by the Assistant Secretary of the Air Force for Acquisition (SAF/AQ) prior to procurement. **(T-1)**.

A6.2.2.2. Air Force will actively monitor Director, National Security Agency initiatives to identify use cases and implementation standards and plans to leverage Trusted Platform Module functionality. **(T-1)**.

A6.2.3. Air Force Information Technology identification and authentication tokens (i.e., Common Access Cards) will be issued in accordance with guidance contained in Air Force Instruction 36-3026_IP, Volume 1, *Identification (ID) Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel,* and DoD Instruction 5200.46, *DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)*. **(T-0)**.

A6.2.4. SAF/CIO A6 has approved the use of the Alternate Logon Token in for circumstances in which a Common Access Card cannot be issued. The Alternate Logon Token is a DoD authorized Public Key Infrastructure hardware token or smart card that can be issued to individuals for logical access to Non-classified Internet Protocol Routing Network. Currently, the Secret Internet Protocol Routing Network is not Alternate Logon Token-compatible. **(T-1)**. Technical Order 31S5-4-7282-1, *Alternate Logon Token (ALT) Issuance Standard Operating Procedures*, is germane.

A6.2.5. The Volunteer Logical Access Credential may be issued to eligible volunteers.

A6.2.6. Air Force Information Technology may be biometrics-enabled where operationally desirable and technically feasible in support of joint military operations in accordance with DoD Directive 8521.01E, *DoD Biometrics*. The following considerations apply:

A6.2.6.1. Biometrics may be incorporated as one authentication factor in a multi-factor access architecture.

A6.2.6.2. All biometric biographic, behavioral, and contextual data collected and maintained by the Air Force must be considered DoD data, and protected in accordance with guidance contained in DoD Directive 8521.01E. **(T-0)**.

A6.2.6.3. Biometric information is considered Personally Identifiable Information, and must be handled and protected in accordance with guidance contained in in accordance with Air Force Instruction 33-332, *Air Force Privacy and Civil Liberties Program*. **(T-0)**.

A6.2.7. Air Force Information Technology identification and authentication mechanisms (Common Access Card and non-Common Access Card) will be managed to ensure that that any credential used for identity authentication is appropriate for the authenticating entity's environment or physical location and the sensitivity level of the information or force protection level of the facility or other resources for which the information system facilitates access or privilege, in accordance with DoD Instruction 8520.03, *Identity Authentication for Information Systems*. **(T-0).**

A6.2.8. Air Force Information Technology that can accessed only through password-based authentication will adhere to the following standards if technically capable:

A6.2.8.1. Each ‘password’ must consist of a passphrase, defined as 4 or more words containing at least 18, but up to 64, total characters. **(T-1)**.

A6.2.8.2. Passphrases must be constructed from a 95-character keyspace: upper case characters, lower case characters, special characters, spaces, and numbers are all allowed. **(T-1)**.

A6.2.8.3. Air Force Information Technology accessed through passphrase-based authenticators must enforce a minimum password life of 90 days, with maximum determined at the command level **(T-3)**; passphrases may be suspended or disabled upon suspicion of compromise, or in response to user re-assignment, departure, extended absence, retirement, or misconduct. Attachment 5, *Account Management*, is germane.

A6.2.8.4. Passphrases must not be reused for a minimum of 5 generations; new passphrases must replace at least 3 words in each generation. **(T-1)**.

A6.2.8.5. All passphrases must be encrypted while in storage or transit. **(T-0)**.

A6.2.8.6. Temporary passwords/passphrases issued for initial logon must be configured for one-time use, requiring an immediate change to a long-term passphrase. **(T-1)**.

A6.2.9. Air Force Information Technology that can accessed only through Personal Identification Number-based authentication will be configured to require at least six digits if technically capable. **(T-0)**.

A6.2.10. Air Force Information Technology must obscure authentication information feedback (e.g., clear text passphrases and Personal Identification Numbers) during the authentication process to protect the information from possible exploitation/use by unauthorized subjects. **(T-1)**.

A6.2.11. Air Force Information Technology must implement mechanisms for authentication to cryptographic modules in accordance with Air Force Manual 17-1302-O, *Communications Security (COMSEC) Operations*, as appropriate. **(T-1)**.

A6.2.12. Air Force Information Technology must uniquely identify and authenticate non-Air Force users (or processes acting on behalf of non- Air Force users). **(T-1)**.

A6.2.12.1. Air Force Information Technology must accept and electronically verify Federal Information Processing Standard Publication 201-2 compliant Personal Identity Verification credentials from other DoD components and federal agencies in accordance with the requirements of Homeland Security Presidential Directive-12, *Policies for a Common Identification Standard for Federal Employees and Contractors*. **(T-0)**.

A6.2.12.2. Air Force Information Technology viewable and/or accessible by the public, and which requires individual authentication must accept only Federal Identity, Credential, and Access Management-approved third-party credentials. **(T-0)**.

A6.2.12.3. Air Force Information Technology viewable and/or accessible by the public, and which requires individual authentication must address open identity management

standards that conform to Federal Identity, Credential, and Access Management -issued implementation profiles of approved protocols (e.g., SAML 2.0, OpenID 2.0). **(T-0)**.

Attachment 7 – Least Privilege and Separation of Duties

A7.1. Overview:

A7.1.1. Least privilege is a control technique intended to ensure that individuals are granted access only to the objects that are required to accomplish their assigned work tasks. Implementing this technique requires privileges be provisioned in accordance with an individuals' level of authority and business or operational mission function. Least privilege principles are applicable across a wide range of technical and operational environments/ situations; these include but are not limited to Air Force Information Technology systems (i.e., networks, databases, operating systems, and applications), financial processes, software development, and system authorization. Segregation of Duties principles are closely related to those of Least Privilege; Segregation of Duties is a control technique that is intended to ensure that no single individual gains excessive control over a critical process.

A7.1.2. Together, Least Privilege and Segregation of Duties help to ensure that no individual or individuals gain excessive control over a critical process to illegally or inappropriately alter results or compromise a critical mission. These controls, when properly implemented and operated, help ensure the integrity of operationally-significant processes, as well as the operation and management of Air Force Information Technology, system development, change management, and authorization processes under the terms of Air Force Instruction 17-101, *Risk Management Framework for Air Force Information Technology (IT)*.

A7.2. Implementation:

A7.2.1. To address these challenges, processes must be designed in a manner that enables or makes possible the implementation of Least Privilege and Segregation of Duties controls. **(T-1)**. In addition, Least Privilege and Segregation of Duties principles and controls must be reflected in the design of access roles and privilege structures. **(T-3)**. The following guidance applies:

A7.2.1.1. Privileges must be assigned so that duties that present a clear conflict of interest are divided among separate, independent personnel, and in a manner that helps prevent an authorized individual or individuals from gaining excessive control over a process to illegally or inappropriately alter results, or that prevents error from being detected through two-person review. **(T-1)**. To this end, the following system support functions must be performed by different individuals **(T-1)**:

A7.2.1.1.1. Information security management

A7.2.1.1.2. System/application design

A7.2.1.1.3. System/application programming

A7.2.1.1.4. Quality assurance/testing

A7.2.1.1.5. Library management/change management

A7.2.1.1.6. Computer operations

A7.2.1.1.7. Production control and scheduling

A7.2.1.1.8. Data control

A7.2.1.1.9. Data security

A7.2.1.1.10. Data administration

A7.2.1.1.11. Network administration

A7.2.1.1.12. Configuration management

A7.2.1.2. No individual will be granted complete control over incompatible transaction processing functions. **(T-1)**. Specifically, the following combination of functions must not be performed by a single individual **(T-1)**:

A7.2.1.2.1. Data entry and verification of data.

A7.2.1.2.2. Data entry and its reconciliation to output.

A7.2.1.2.3. Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information).

A7.2.1.2.4. Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).

A7.2.1.3. Procedures and standards specifying high-risk privilege combinations and incompatible duties must be developed to address Least Privilege and Segregation of Duties requirements in the above listed process areas, and promulgated throughout the organization. **(T-3)**.

A7.2.1.4. Non-privileged users must not be allowed to execute privileged functions, to include disabling, circumventing, or altering implemented security safeguards and countermeasures. **(T-1)**.

A7.2.1.5. Privileged function execution must be captured in system-level audit vent logs, and these logs must be reviewed at the responsible management level to detect potential abuses. **(T-1)**. Audit logs must be retained as Configuration Items. **(T-2)**.

A7.2.1.6. Users who are provisioned with Air Force Information Technology system accounts or roles with access to security functions or security-relevant information must be provisioned with, and required to use, a non-privileged account or role when accessing nonsecurity functions. **(T-0)**.

A7.2.1.7. Access to:

A7.2.1.7.1. Software development,

A7.2.1.7.2. Software test, and

A7.2.1.7.3. Software production environments must be segregated; users with access to one environment must not be privileged to access or migrate code to either of the other two environments without formal management approval. **(T-1)**.

A7.2.1.8. Procedures must be developed to maintain auditability of privilege use in cases where emergency access is authorized; evidence of emergency access approvals and provisioning must be maintained as CIs. **(T-2)**.

A7.2.1.9. The design and implementation of Least Privilege and Segregation of Duties procedures and standards must be periodically reviewed to ensure that they are in place and operating as intended; evidence of having done so (e.g., memos for the record, emails, etc.), must be maintained as Configuration Items. **(T-2)**.

A7.2.1.10. User roles and permissions/privileges must be explicitly detailed in Block 13 of the System Authorization Access Request (DD 2875), specifying as appropriate, each users privilege to access key control points in the business/mission process. **(T-1)**. This includes:

A7.2.1.10.1. Privileges to authorize, initiate, approve, or reconcile financial and financially-significant transactions [1].

A7.2.1.10.2. Privileges to access to security functions deployed in hardware, software, and firmware and security-relevant information.

A7.2.1.10.3. Privileges to migrate software between development, test, and production environments; authority to promote code to production must be restricted to the fewest practical number of personnel.

A7.2.2. In cases where a Program Manager has determined that technical or resource constraints make it difficult or impractical to limit privileges or maintain a strict separation of duties, compensating controls must be employed to mitigate risk. Such measures must be reviewed by system/application management and the cognizant Information System Security Manager, and approved by the cognizant Authorizing Official. Examples of commonly accepted mitigation measures include:

A7.2.2.1. Rotation of duties among personnel;

A7.2.2.2. Increased hands-on supervision;

A7.2.2.3. Enforced vacations;

A7.2.2.4. Having a manager perform one aspect of the transaction (e.g. making the cash deposits, approving invoices, etc.);

A7.2.2.5. Active review by management of financial data and reports (e.g. reconciliations, voucher status report, appropriation status reports.

[1] E.g.: defining or updating Master Control data, altering a database schema, creating general ledger (G/L) accounts, and/or altering data outside the application

Attachment 8 – Authorized Use of Personal Devices

8.1. Overview: The growing prominence of mobile computing capabilities and demand for expanded use of personally-owned (i.e., non-Government Furnished Equipment) information technology is transforming how the Air Force executes its missions, connects with itself and mission partners, communicates up and down the chain of command, and supports its personnel. In support of these trends and the advancement of Air Force information technology services, this Attachment provides information and guidance on the use of personally-owned electronic devices with the Air Force Information Network.

8.2. Implementation:

A8.2.1. All Air Force personnel using personally-owned electronic devices in Air Force spaces must comply with the requirements and responsibilities cited below:

A8.2.1.1. Personally-owned electronic device users must sign an acceptable use agreement (Air Force Form 4433) before use in unclassified Air Force spaces. **(T-3)**.

A8.2.1.2. Personally-owned electronic devices (if approved), must obtain Authorizing Official approval prior in order to receive, process, and transmit Department of Defense information, or to operate on or with Air Force Information Technology. **(T-2).**

A8.2.1.3. Personally-owned electronic devices are prohibited from being introduced into any space where classified information is processed, stored, displayed, discussed, or transmitted. **(T-3).**

A8.2.1.4. Unclassified government cell phones and all personally-owned laptops, tablets, cell phones, smart watches, music players, wireless keyboards and pointing devices, wireless headphones, and printers must be secured outside of classified spaces. **(T-3)**. Lacking secure storage, devices with cellular and wireless transmit capabilities may be brought into classified spaces, but must be disabled or powered down prior to entry in accordance with local policy. **(T-3)**.

A8.2.1.4.1. Personally-owned electronic devices are permitted in Air Force spaces where unclassified and/or sensitive (see Attachment 3 to this Instruction) information is processed, stored, displayed, discussed, or transmitted, subject to the following restrictions; personally-owned electronic devices must:

A8.2.1.4.1.1. Be on an approved list of devices. **(T-1)**. At minimum, they must be commercially obtained in the U.S. or through a U.S. military exchange, and assigned a Federal Communication Commission Identifier denoting compliance with the limits for a Class B digital device designated by the Federal Communication Commission, pursuant to Part 15 of the Federal Communication Commission Rules, per Federal Communications Commission Office of Engineering and Technology Bulletin Number 62, *Understanding the FCC Regulations for Computers and Other Digital Devices*.

A8.2.1.4.1.1.1. Devices allowed in classified spaces include hearing aids, pacemakers and other implanted medical devices, or personal life support systems. Exercise trackers may be permitted at the discretion of the senior officer in each classified facility/suite. **(T-3).**

A8.2.1.4.1.1.2. Devices disallowed in classified spaces include unclassified government cell phones and all personally-owned laptops, tablets, cell phones, pagers, Global Positioning System transceivers, smart watches, music players, wireless keyboards and pointing devices, wireless headphones, and printers. **(T-3).** Such devices must be secured outside of classified spaces in accordance with local policy.

A8.2.1.4.1.2. In accordance with the requirements of Attachment 4, *Access Control*, and Attachment 6, *Identification and Authentication*, control access to information and capabilities with the strongest available mechanism; 2-factor authentication, OR a strong password, OR a PIN of at least six characters. Control access to information and capabilities with the strongest available mechanism **(T-1)**;

A8.2.1.4.1.3. Have installed only whitelisted applications and receive only updates that do not add any prohibited features or capabilities. **(T-3)**.

A8.2.1.4.1.4. Partition Air Force and other government data from personal data, when technically feasible. **(T-2)**.

A8.2.1.4.1.5. Have up-to-date anti-malware software installed, where such capabilities exist. **(T-2)**.

A8.2.1.4.1.6. Be surrendered to Air Force cybersecurity staff periodically for compliance monitoring when requested. **(T-2)**.

A8.2.1.5. Use of personally-owned electronic devices is permitted primarily to facilitate the conduct of government/Air Force business. Limited personal use may be allowed in accordance with local command policies and standards, however, authorized users who are determined to be abusing personal-use privileges will have their access rights suspended or removed. **(T-1).**

A8.2.1.6. Personally-owned electronic devices connections to the Air Force segment of the Non-Secure Internet Protocol Network, must be encrypted using Air Force-approved software, e.g., Virtual Private Network security software, in accordance with DoD Directive 8100.01 and DoD Instruction 8520.03. **(T-0).**

A8.2.1.7. Air Force Information Network-connected devices, including personally-owned electronic devices, are subject to monitoring for compliance with applicable policies and standards in DoD Instruction 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations*, and Air Force Instruction 17-712, *Public Key Infrastructure and Public Key Enabling.* **(T-1).**

Attachment 9 – Specialized Cybersecurity and Communications Security Publications

A9.1. Overview: Specialized publications include specialized Communications Security, Ports, Protocols, and Services Management, and TEMPEST publications that implement Committee on National Security Systems, National Institute for Standards and Technology, Department of Defense, and National Security Agency-issued cybersecurity policies, directives, instructions, standards, guidance, manuals, and technical information. These documents remain authoritative until their guidance is incorporated into other publications, at which time they will be rescinded.

A9.2. Implementation

A9.2.1. Obtaining Cryptologic and Cyber Systems Division publications:

A9.2.1.1. Order Air Force communications security publications through the Communications Material Control System.

A9.2.1.2. Obtain Limited Maintenance Manuals by emailing a request to CCSD/HNC-PSLT at LMM@us.af.mil. Unclassified Methods and Procedures Technical Orders are maintained in the Enhanced Technical Information Management System, available via the Air Force Portal.

A9.2.2. Accessing Air Force Systems Security Instruction Publications.

A9.2.2.1. Air Force Systems Security Instructions are no longer created or updated and the relevant content is transitioning into Air Force Manuals or Methods and Procedures Technical Orders, if required.

A9.2.2.2. For Official Use Only communications security Air Force Systems Security Instructions are strictly controlled and only available to Communications Security Management System account holders at https://cs3.eis.af.mil/sites/OO-SC-CA-11/default.aspx.

A9.2.2.3. Classified Communications Security Air Force Systems Security Instructions are available upon request by sending an email via the SECRET Internet Protocol Router Network to Air Force Space Command, Cyberspace Support Squadron at usaf.scott.afspc-cyss.mbx.af-comsec-field-support@mail.smil.mil.

A9.2.2.4. Unclassified TEMPEST and Ports, Protocols and Services Management Air Force Systems Security Instructions are located on the Air Force Information Assurance Collaborative Environment SharePoint site at https://cs2.eis.af.mil/sites/10060/Publications/Forms/AllItems.aspx.

Questions regarding this policy can be forwarded to the SAF/CIO A6 Cybersecurity Division, usaf.pentagon.saf-cio-a6.mbx.a6sc-workflow@mail.mil. This Memorandum becomes void after one-year has elapsed from the date of this Memorandum, or upon publication of an Interim Change or rewrite of the affected publication, whichever is earlier.

BRADFORD J. SHWEDO, Lt Gen, USAF
Chief of Information Dominance and
Chief Information Officer

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-200

31 AUGUST 2015
Certified Current 16 February 2016
Communications and Information

AIR FORCE CYBERSECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF CIO/A6SC

Certified by: SAF/CIO A6S
(Col Mary Hanson, AF SISO)

Supersedes: AFI 33-200, 23 December 2008; AFI 33-220, 21 November 2007

Pages: 50

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Assurance (IA) Program*, and establishes Air Force (AF) cybersecurity requirements for compliance with: Committee on National Security Systems Instruction (CNSSI) No. 4005, (FOUO) *Safeguarding Communications Security(COMSEC) Facilities and Materials*; Committee on National Security Systems Instruction (CNSSI) No. 4016, (FOUO), *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, CNSSP -11*; Department of Defense (DoD) Chief Information Officer (CIO) Memorandum, *Commercial Mobile Device (CMD) Interim Policy*; DoD Directive (DoDD) 8100.2, *Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*; DoD Instruction (DoDI) 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*; DoDI 8500.01, *Cybersecurity*; DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*; DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*; DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*; DoDI 8540.01. *Cross Domain (CD) Policy;* DoDI 8520.03, *Identity Authentication for Information Systems*; DoDI O-8530.2, *Support to Computer Network Defense (CND)*; DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM);* DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System;* DoDI 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*; and DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*. This instruction is consistent with Chairman Joint Chiefs of Staff Instruction CJCSI 6510.01F, *Information Assurance (IA) and Computer Network Defense (CND)*; CJCSI 6211.02D, *Defense Information Systems network (DISN) Responsibilities* and; Chairman Joint Chiefs of Staff

Manual (CJCSM) 6510.01A, *Information Assurance (IA) and Computer Network Defense (CND) Volume 1 (Incident Handling Program)*. This instruction applies to all AF military, civilian, and contractor personnel under contract by DoD, regardless of Air Force Specialty Code (AFSC), who develop, acquire, deliver, use, operate, or manage AF Information Technology (IT). This instruction applies to the Air National Guard (ANG) and Air Force Reserve Command (AFRC). The term major command (MAJCOM), when used in this publication, includes field operating agencies (FOA) and direct reporting units (DRU). Use of extracts from this instruction is encouraged. CNSSI 4009, *National Information Assurance (IA) Glossary*, explains other terms. Direct questions, comments, recommended changes, or conflicts to this publication through command channels using the AF Form 847, *Recommendation for Change of Publication*, to SAF/CIO A6. Send any supplements to this publication to SAF/CIO A6 for review, coordination, and approval prior to publication. Unless otherwise noted, the SAF/CIO A6 is the waivering authority to policies contained in this publication. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFMAN 33-363, *Management of Records*, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This document is substantially changed and should be reviewed in its entirety. The change is a result of a DoD policy directive update and establishes the AF Cybersecurity program and risk management framework as an essential element to accomplishing the AF mission.

Chapter 1

GENERAL INFORMATION

1.1. Introduction. This AFI provides general direction for implementation of cybersecurity and management of cybersecurity programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the confidentiality, integrity, and availability (CIA) of AF IT and the information they process. This AFI ensures the use of appropriate levels of protection against threats and vulnerabilities, helps prevent denial of service, corruption and compromise of information, and potential fraud, waste, and abuse of government resources.

1.1.1. The AF cybersecurity program incorporates strategy, policy, awareness/training, assessment, authorization, implementation and remediation.

1.1.2. The cybersecurity discipline aligns with the AF Cybersecurity strategy key concept that total risk avoidance is not practical and therefore risks assessment and management is required.

1.1.3. Cybersecurity encompasses the following disciplines/functions: Air Force Risk Management Framework (RMF), IT controls/countermeasures, Communications Security (COMSEC), Computer Security (COMPUSEC), TEMPEST (formerly known as Emissions Security [EMSEC]), AF Assessment and Authorization (A&A) (formerly known as Certification and Accreditation Program [AFCAP]), and Cybersecurity Workforce Improvement Program (WIP).

1.2. Applicability. This publication is binding on all military, civilian and contractors or other persons through the contract or other legally binding agreement with the Department of the Air Force, who develop, acquire, deliver, use, operate, or manage AF IT. This publication applies to all AF IT used to process, store, display, transmit, or protect AF information, regardless of classification or sensitivity. AF IT includes but is not limited to: Information Systems (Major applications & Enclaves), Platform Information Technology (PIT) & PIT systems, IT Services (Internal & External), and IT Products (Software, Hardware, Applications).

1.2.1. More restrictive Federal, DoD, and Director of National Intelligence (DNI) directive requirements governing Special Access Program (SAP) information take precedence over this publication. The latest version of all publications (e.g., Federal, Joint, DoD, AF) referenced within this publication are to be used.

1.2.2. This publication and implementation guidance identified within is not applicable to Intelligence Community ISs to include Sensitive Compartmented Information (SCI) ISs. Refer to the Intelligence Community (IC) Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation and or the Unified Cross Domain Services Management Office (UCDSMO) as applicable.

1.2.3. Authority for AF space systems rests with Air Force Space Command (AFSPC) as delegated by US Strategic Command (USSTRATCOM). AF space systems generally follow AF Cybersecurity policy and processes; where exceptions exist, this instruction is annotated accordingly. NOTE: Non-AF space systems follow cybersecurity policy and guidance in DoDI 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense.

1.2.4. Effective implementation and resultant residual risk associated with cybersecurity controls is assessed, documented, and mitigated according to DoDI 8510.01, DoD Risk Management Framework (RMF), Air Force Manual (AFMAN) 33-210, Air Force Assessment and Authorization Program, and the AF RMF Knowledge Service, for inclusion in the AF Information Technology (IT) A&A package.

1.3. Objectives. The objective of the AF Cybersecurity Program is to manage the risk presented by adversary cyber capabilities (purposeful attacks) and intelligence, environmental disruptions, human or machine errors, and to maintain mission survivability under adversary offensive cyber operations. The AF implements and maintains the Cybersecurity Program to adequately secure its information and IT assets. The Cybersecurity Program:

1.3.1. Ensures AF IT operate securely by protecting and maintaining IS / PIT resources and information processed throughout the system's life cycle.

1.3.2. Protects information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

1.3.3. Leverages the multi-tiered organization-wide risk management approach defined in NATIONAL Institute of Standards and technology (NIST) Special Publication (SP) 800-39, Managing Information Security Risk (See figure 1.1).

1.3.3.1. Tier 1 – Organization: Risk management at this tier is performed through cybersecurity governance bodies at the AF enterprise level.

1.3.3.2. Tier 2 – Mission/Business Process: risk management at this tier is performed by mission owner level and is informed by the risk context, risk decisions, and risk activities at Tier 1.

1.3.3.3. Tier 3 – Information System: risk management at this tier is performed by individuals responsible for the management of individual IT and is guided by the risk context, risk decisions and risk activities at Tiers 1 and 2.

Figure 1.1. Tiered Risk Management Approach (NIST SP 800-39).

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO A6) will develop strategies, policy and programs to integrate warfighting and combat support capabilities according to DoDI 8500. 01 and AFPD 33-2. SAF/CIO A6 will:

2.1.1. Oversee the establishment of risk tolerance and baseline cybersecurity controls for the AF IT. SAF CIO A6 will provide guidance to organizations on how to implement solutions for operational requirements exceeding the established National, DoD, Joint Chiefs of Staff (JCS), AF baseline cybersecurity controls for IT and remain within established risk tolerance levels

2.1.2. Maintain visibility of assessment and authorization status of AF IT through automated assessment and authorization tools or designated repositories for the AF in support of DoD CIO and Principle Authorizing Officials (PAO) IAW DoDI 8500.01, Cybersecurity.

2.1.3. Provide guidance to organizations on how to implement solutions for operational requirements exceeding the established National, DoD, Joint Chiefs of Staff (JCS), AF baseline cybersecurity controls for IT and remain within established risk tolerance levels.

2.1.4. Define cybersecurity performance measures and metrics to identify enterprise-wide cybersecurity trends and status of mitigation efforts.

2.1.5. On behalf of the SECAF, and IAW AFPD 33-2, appoint all Authorizing Officials (AO).

2.1.6. Appoint an Air Force Senior Information Security Officer (SISO) to direct and oversee the Air Force Cybersecurity Program.

2.1.7. IAW AFI 33-401, Air Force Architecting, appoint the AF Chief Architect with responsibility for the AF Cybersecurity Architecture.

2.1.8. Serve as the Mission Area Owner (MAO) for the Enterprise Information Environment Mission Area (EIEMA).

2.1.9. Chair the Air Force AO Summit.

2.1.10. Represent the EIEMA in the Air Force AO Summit.

2.1.11. Provide AF Enterprise oversight of the Air Force Information Technology Asset Management (ITAM) program.

2.2. Assistant Secretary of the Air Force (Acquisition) (SAF/AQ) will:

2.2.1. Build cybersecurity into all acquisitions by ensuring all cybersecurity requirements are implemented in all phases and contracts for research, development, test, and evaluation of IT.

2.2.2. Provide streamlined guidance to enable Program Executive Officers (PEO) and Program Managers (PM) to adhere to the mandated standards outlined in this instruction, DoDI 8580.1, DoDI 8581.1, DoDI 8510.01, AFMAN 33-152, and the A&A requirements of AFMAN 33-210.

2.2.3. Ensure contracts include appropriate Defense Federal Acquisition Regulation Supplement (DFARS) clauses for safeguarding unclassified DoD information on non-DoD ISs IAW DoDI 8582.01 and DFARS 204.7304 as applicable.

2.2.4. For all space acquisitions, ensure cybersecurity requirements are implemented in all phases of acquisitions according to the provisions in DoDI 5000.02, Operation of the Defense Acquisition System. SAF/AQ will provide streamlined guidance to enable each program and system under its span of control to develop a cybersecurity strategy meeting the requirements of this instruction, DoDI 5000.02, and DoDI 8580.1, and AFMAN 33-407, Air Force Clinger-Cohen Act (CCA) Compliance Guide.

2.2.5. Manage the process for preparing and reviewing AF acquisition program strategies and ensure cybersecurity has been appropriately addressed.

2.2.6. Represent the AF on policy and procedural matters regarding cybersecurity in the acquisition system.

2.2.7. Coordinate with USAF/A2 to ensure Intelligence acquisition programs address cybersecurity life cycle requirements. SAF/AQ will coordinate with USAF/A2 assigning AF PM representatives for Intelligence systems, equipment, networks, or services on the Air Force Information Network (AFIN) or utilizing AFIN capabilities that were developed and/or acquired by non-AF entities.

2.3. Air Force Office of Special Investigations (AFOSI) will:

2.3.1. AFOSI is the office of primary responsibility (OPR) for on-hook telephone technical security matters, to include providing guidance for installing and operating telephone systems within the Air Force, and department of defense facilities occupied by Air Force personnel.

2.3.2. Provide Air Force representation to the U.S. Government intelligence community's National Telephone Security Working Group (NTSWG). **(T-0)**. The group is the primary technical and policy resource in the U.S. intelligence community for all aspect of the Technical Surveillance Countermeasures (TSCM) program involving telephone systems in areas where sensitive government information is discussed.

2.3.3. Examine the TSCM needs of the Air Force and tailor Air Force telephone security standards to those established by the NTSWG. **(T-0)**.

2.3.4. Provide guidance to Air Force organization on selecting local equipment for installing telephone systems in sensitive discussion areas in conjunction with the host base Communications and Information Systems Officer (CSO) (AFMAN 33-145, Collaboration Services and Voice Systems Management) in accordance with CNSSI No. 5006, National Instruction for Approved Telephone Equipment, and The Defense Information Systems Agency (DISA) Approved Products List Integrated Tracking System (UC system acquisition). **(T-0)**.

2.3.5. Determine the effectiveness and applicability of protective security devices and TSCM procedures for qualified facilities; when warranted provide technical threat information and briefings concerning telephone systems and the countermeasures intended to nullify existing threats. **(T-0)**. Further information on requesting TSCM services or threat briefing is contained in AFI 71-101, Volume 3, The Air Force Technical Surveillance Countermeasures Program.

2.4. Mission Area Owner (MAO). A MAO is appointed for the Air Force portion of each of the DoD MAs. MAOs will:

2.4.1. Oversee and establish direction for the strategic implementation of cybersecurity and risk management within their MAs. **(T-0)**.

2.4.2. Assist the SAF/CIO A6 and the AF SISO in assessing the effectiveness of AF cybersecurity. **(T-1)**.

2.4.3. Coordinate with the DoD PAO for cybersecurity and risk management within their MAs. **(T-0)**.

2.4.4. Represent the interest of the MA, as defined in Reference DoDD 8115.01, Information Technology Portfolio Management, and, as required issue authorization guidance specific to the MA, consistent with this instruction. **(T-0)**.

2.4.5. Resolve authorization issues within their respective MAs and work with other MAOs to resolve issues among MAs, as needed. **(T-0)**.

2.4.6. Nominate AOs for MA IS and PIT systems supporting MA COIs specified in Reference DoD 8320.02, in coordination with SAF/CIO A6, consistent with this instruction. **(T-1)**. SAF/CIO A6 will appoint those nominated by the MAO.

2.4.7. Designate information security architects or IS security engineers for MA segments (overlapping spans of influence (enclaves)) or systems of systems, as needed. **(T-1)**.

2.4.8. Work with the AF SISO and other MAOs to ensure cybersecurity checks and balances occur through the appropriate mission area governance boards. **(T-1)**.

2.5. Twenty-Fourth Air Force (24AF (AFCYBER)) will:

2.5.1. Serve as the single point of contact for processing and supporting AF cybersecurity-related intelligence requests from AF and DoD intelligence entities (e.g., threat assessment against the AFIN) for the AFIN. 24 AF (AFCYBER) will provide SAF/CIO A6 Staff with courtesy copies of requests and responses for assessment of impact on the AF cybersecurity Program.

2.5.2. Coordinate with Joint and Defense-wide program offices to ensure interoperability of cybersecurity solutions across the DODIN.

2.5.3. Provide support to national, DoD, and AF level Technical Advisory Groups (TAG) (i.e., AFIA TAG, RMF TAG, DoD PPS TAG, etc.), as requested by SAF/CIO A6.

2.5.4. Oversee, manage, and control AF enclave boundary defense activities, measures, and operations.

2.5.5. Issue time compliance technical orders and modification kits for cybersecurity and cybersecurity-enabled products or components of AF ITs.

2.5.6. Ensure Ports Protocols and Services (PPS) requirements for the AFIN are limited to only those required for official use with proper approval, PPS's not properly approved follow the deny by default, allow by exception access philosophy, and that PPS information is validated annually.

2.6. AF Senior Information Security Officer (SISO) will develop, implement, maintain, and enforce the AF Cybersecurity Program. The AF SISO will direct and coordinate any associated budgets and advocate for AF-wide cybersecurity solutions through the planning, programming, budget and execution process on behalf of the SAF/CIO A6 according to DoDI 8500.01, DoDI 8510.01, AFPD 33-2, and AFMAN 33-210. The SISO is referred to as Senior Agency Information Security Officer [SAISO] or Chief Information Security Officer [CISO] in CNSSI 4009. The AF SISO will:

2.6.1. Be a DoD official (O-6 or GS-15 at a minimum), and a United States citizen.

2.6.2. Complete training and maintain cybersecurity certifications IAW AFMAN 33-285, Cybersecurity Workforce Improvement Program.

2.6.3. Monitor, evaluate, and provide advice to the SAF/CIO A6 regarding AF cybersecurity posture.

2.6.4. Serve as the AF CIO's primary liaison to DoD SISO, Component SISO's, MAJCOM Cybersecurity Offices, AF AOs, and SCAs.

2.6.5. In coordination with the SAF/CIO A6 and AO's, ensure cybersecurity risk posture and risk tolerance decisions for AF IT meet mission and business needs while also minimizing the operations and maintenance burden on the organization. The AF SISO will represent the AF at Federal, DoD, and Joint cybersecurity steering groups and forums.

2.6.6. Ensure that IT guidelines are incorporated into acquisition, implementation, and operations and maintenance functions.

2.6.7. Provide direction on how cybersecurity metrics are determined, established, defined, collected, and reported for compliance with statutory, DoD, Joint, and AF policies and directives.

2.6.8. Appoint Security Control Assessors (SCAs) for all AF IT (excluding Special-Access Program/Special Access Required [SAP/SAR], IC, Space, NC3, and Medical).

2.6.9. Perform as the SCA or formally delegate the security control assessment role for governed information technologies.

2.6.10. Provide guidance and direction on Agent of the Security Control Assessor (ASCA) establishment in support of Assessment and Authorization (A&A) requirements.

2.6.11. Oversee establishment and enforcement of the A&A process, roles, and responsibilities; review approval thresholds and milestones within the AF A&A Program.

2.6.12. Chair the Air Force Cybersecurity Risk Management Council (AFCRMC).

2.6.13. Adjudicate IT determinations, in coordination with the Air Force Risk Management Council, when there is a conflict in the IT determination process.

2.6.14. Appoint in writing the AF Certified TEMPEST Technical Authority (AF CTTA).

2.6.15. Appoint AF members to the DoD RMF TAG.

2.6.16. Review and approve Cybersecurity Strategies for all AF IT IAW DoDI 5000.02 and AFMAN 33-407, AF Clinger-Cohen Act (CCA) Compliance Guide. The approval of the Cybersecurity Strategies cannot be delegated.

2.6.17. Review and approve Privacy Impact Assessments (PIAs) submitted IAW AFI 33-332, The AF privacy and Civil Liberties Program. The approval of the PIA may be not be delegated.

2.6.18. Approve National Security System (NSS) designations for AF IT.

2.6.19. Approve Defense Industrial Base Cybersecurity/Information Assurance (DIB/CS/IA) Damage Assessment Reports (as needed) IAW DoDI 5205.13.

2.6.20. Ensure AF RMF guidance is posted to the DoD Component portion of the KS, and is consistent with DoD policy and guidance.

2.6.21. Validate and prioritize (with the support of the AF Risk Management Council (AFRMC)) all AF cryptographic certification requests prior to submission for NSA action.

2.7. Air Force Office of Cyberspace Strategy and Policy (SAF CIO A6S) will:

2.7.1. Provide cyberspace policy, guidance, & oversight. SAF CIO A6S will inform Headquarters United States Air Force, and MAJCOMs about changes to DoD and AF cybersecurity policies and procedures in accordance with HAFMD1-26 Chief, Information Dominance and Chief Information Officer.

2.7.2. Ensure AF acquisition guidance reflects national, federal, DoD, and AF cybersecurity policy and procedures.

2.7.3. Develop and evaluate cybersecurity performance measurements for compliance with statutory, DoD, Joint, and AF policies and directives.

2.7.4. Establish and enforce the RMF process, roles, and responsibilities; review approval thresholds and milestones within the AF RMF Program.

2.7.5. Provide AF IT PEO's guidance on completion and submission of Cybersecurity Strategies and submit for AF SISO approval.

2.7.6. Collect and report cybersecurity management, financial, and readiness data to meet DoD cybersecurity and Office of Management and Budget (OMB) reporting requirements.

2.7.7. Serve as the single cybersecurity coordination point for joint or Defense-wide programs that are deploying IT (guest systems) to AF enclaves.

2.7.8. Participate in Federal, DoD and Joint cybersecurity and RMF technical working groups and forums (e.g. RMF TAG, DSAWG).

2.7.9. Develop and implement AF cybersecurity requirements planning, programming, budgeting, and execution in the AF budget process in compliance with SISO direction. Through the Air Force budget request, SAF CIO A6S will advocate for cybersecurity funding and manning with the Office of the Secretary of Defense and Congress.

2.7.10. Establish and maintain cybersecurity checklists for use with the AF Inspection Systems, currently the Management Internal Control Toolset (MICT) in accordance with AFI 90-201 Air Force Inspection System.

2.7.11. Develop concepts and establish strategy for integrated support and configuration management of cybersecurity equipment.

2.7.12. Oversee, plan, implement, manage, and support the COMSEC aspects of programs, including centralized record maintenance of COMSEC equipment, components, and material.

2.7.13. Carry out Federal Information Security Management Act of 2002 (FISMA)-related CIO responsibilities.

2.7.14. Provide detailed information on the FISMA requirements via the annual AF FISMA Reporting Guidance.

2.7.15. Manage the annual assessment of the AF Cybersecurity Programs as required by FISMA. Requests, through channels, support from AF organizations. Organizational support allows the AF SISO to answer the annual FISMA report questions posed by the OMB.

2.7.16. Ensure cybersecurity requirements are addressed and visible in all investment portfolios and investment programs according to AFI 33-401, Air Force Architecting, and AFMAN 33-210

2.7.17. Implement and enforce the education, training, and certification of AF cybersecurity professionals and users according to DoD 8570.01-M, Information Assurance (IA) Training, Certification, and Workforce Management, and AFMAN 33-285.

2.7.18. Coordinate Inspector General (IG) inspections and associated responsibilities according to and AFI 90-201.

2.7.19. Collect and report on qualification metrics and submits reports to the DoD CIO as directed such as for Federal Information Security Management Act (FISMA) reporting, standardizing reporting across Air Force.

2.7.20. Review and provide guidance in support of MAJCOM or equivalent provided commercial internet waivers and facilitates presentation to the DoDIN waiver panel; is a voting member of the DoDIN waiver panel. For additional information, AFI 33-115 and AFMAN 33-282.

2.7.21. Review Cross Domain Solution (CDS) requests and presents to the Defense Security Accreditation Working Group (DSAWG) for approval.

2.7.22. Manage the implementation of policy and standardized procedures to catalog, regulate, and control the use and management of ports, protocols, and services (PPS) in IT and applications IAW DoDI 8551.01.

2.7.23. Serve as the AF Public Key Infrastructure (PKI Management Authority (PMA). SAF CIO A6S will direct policy, requirements, and implementation of PKI integration across all AF networks. SAF CIO A6S will participate in DoD and Federal working groups and forums involved in PKI and IdAM, and is the AF OPR to DoD, NSS, and Federal PKI and Identity and Access Management (IdAM) groups.

2.7.24. Represent the AF as a voting member on DoD PPS Configuration Control Boards (CCB). Designates AF A6S as primary and one or more alternate voting representatives for the DoD PPS CCB.

2.7.25. Designate a primary and one or more alternate representatives for the DoD PPS TAG.

2.7.26. Designate points of contact to register the PPS used by AF IS in the DoD PPS Registry (also known as DoD PPS Database) according to this instruction and DoD policy.

2.7.27. Manage PPS procedures for the AF according to this instruction, DoD guidance, and USCYBERCOM orders and directives. Responsibilities include advocating issues from customers with Air Staff and the DoD PPS Program Manager at the Defense Information Systems Agency (DISA); providing guidance and support to customers; and processing waiver, deviations, and exceptions.

2.7.28. Establish a Defense Industrial Base Cyber Security/ Information Assurance (DIB CS/IA) Program Office. The DIB CS/IA Program Office works cooperatively with participating Cleared Defense Contractors (CDCs) to enhance their ability to safeguard DoD information residing on or transiting DIB unclassified networks IAW DoDI 5205.13, Defense Industrial Base Cyber Security/Information Assurance Activities. In accordance with DoDI 5205.13, the AF established the AF Damage Assessment Management Office (AF DAMO) within SAF/CIO A6.

2.7.29. The AF DAMO will conduct damage assessments on data compromised as a result of adversary intrusions into those contractor networks. AF DAMO determines the extent of intelligence obtained by adversary cyber intrusions into DIB networks, and assesses the overall impact of the data loss on current and future weapons programs, scientific and research projects, and warfighting capabilities.

2.7.30. Set policy for managing AF electronic (EM) spectrum use to support the AF mission and exercise control over the frequency management process IAW AFI 33-580, Spectrum Management

2.7.31. Upon request from the AF SISO, AF functional authorities and MAJCOMs are required to provide appropriate programmatic, operational, and technical SMEs, intelligence analysts, or cyber forces to assess the compromised information as part of Integrated Process Teams (IPTs). All IPTs convene at the DoD Cyber Crime Center (DC3) in Linthicum, MD, where AF DAMO personnel assist the IPT in the damage assessment process. The participants provide expert opinion on the extent of damage caused as a result of the compromise and make recommendations on mitigation efforts required due to the loss of that information. Damage assessment reports are drafted for each case and disseminated to the appropriate AF program offices, agencies, and stakeholders for review and possible mitigation actions.

2.8. Authorizing Official (AO). The AO is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The AO renders authorization decisions for DoD ISs and PIT systems under their purview in accordance with DoDI 8510.01. A current listing of AOs is available on the AF Cybersecurity Knowledge Service located at: **https://cs1.eis.af.mil/sites/SAFCIOA6/A6S/afcks/Compliance/AFAAP/SitePages/Home.aspx**. The AO will:

2.8.1. Be appointed from senior leadership positions within business owner and mission owner organizations to promote accountability in authorization decisions that balance mission and business needs and security concerns/risks.

2.8.2. Be a DoD official (O-7 or SES at a minimum), and be a United States citizen.

2.8.3. Complete AF AO training IAW AFMAN 33-285.

2.8.4. Be appointed by SAF CIO/A6 in coordination with the appropriate MAO. The appointment grants authority to authorize IS and PIT systems within the authorization boundary as needed.

2.8.5. Not delegate ATO granting authority. **(T-1)**.

2.8.6. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program.

2.9. AO Designated Representative (AODR) will:

2.9.1. Complete AO training and maintain cybersecurity certifications consistent with duties and responsibilities of an SCA and IAW AFMAN 33-285. **(T-1)**.

2.9.2. Perform responsibilities as assigned by the AO. NOTE: AODR's may perform any and all duties of an AO except for accepting risk by issuing an authorization decision. **(T-1)**.

2.9.3. Make recommendations to the AO to approve ATO based on input from RMF team members, and other AOs and AODRs. **(T-1)**.

2.9.4. Be appointed by the AO, and, at a minimum, be an O-5 or GS-14. **(T-1)**.

2.10. Security Control Assessor (SCA).

2.10.1. The SCA is the senior official having the authority and responsibility for the certification of all ISs and PIT systems governed by the Air Force.

2.10.2. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program.

2.11. Security Controls Assessor Representative (SCAR) will:

2.11.1. Complete training and maintain appropriate cybersecurity certification IAW AFMAN 33-285. It is highly recommended SCARs complete both the AO training module and attain the CNSSI 4016 certificate for supplemental training. Proof of training (e.g. certificate) is included as an artifact to the IS's or PIT system's A&A package.

2.11.2. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program

2.12. Agent of the Security Controls Assessor (ASCA). The ASCA is a licensed organization which may be contracted by the PM to assist in certification activities and will:

2.12.1. Report directly to the SCA for guidance related to validation activities and procedures. **(T-1)**.

2.12.2. Maintain ASCA license IAW SISO guidance and the ASCA licensing guide. **(T-1)**.

2.12.3. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program

2.13. Information System Owners (ISO). Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information or PIT system. An ISO will be appointed in writing for every IS and PIT System. **(T-1).** For those systems that are Air Force-wide systems (e.g., AFNET, LOGMOD, etc.), they will be appointed

by the HAF/SAF 3-letter responsible for the capability. For MAJCOM, base-level IS/PIT systems, and base enclaves, the appropriate MAJCOM 2-letter will appoint the ISO. No further appointment is necessary. The ISO will:

2.13.1. Identify the requirement for IT and requests funds, operates and maintains the IT in order to enhance mission effectiveness. (NOTE: Do not confuse this with the ISO role in TEMPEST.) **(T-2)**.

2.13.2. Identify, implement, and ensure full integration of cybersecurity into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, operation, and sustainment. **(T-0)**. Reference DoDI 8510.01, AFI 63-101, and AFMAN 33-210 for guidance.

2.13.3. Develop, maintain, and track the security plan for assigned IS and PIT systems. **(T-1)**.

2.13.4. Develop and document a system-level continuous monitoring (CM) strategy to monitor the effectiveness of security controls employed within or inherited by the system, and monitoring of any proposed or actual changes to the system and its environment of operation. **(T-1)**. The ISO must ensure the strategy includes the plan for annual assessments of a subset of implemented security controls, and the level of independence required of the assessor (e.g., SCA or ASCA). **(T-1)**.

2.13.5. Ensure the PMO is resourced with individuals knowledgeable in all areas of cybersecurity to support security engineering and security technical assessments of the IS or PIT systems for the SCA's authorization determination, AOs authorization decision, and other security related assessments (e.g., Financial Improvement and Audit Readiness (FIAR) IT testing, Inspector General audits). (T-1).

2.13.6. Ensure that applicable CTO's are received and acted upon per the CTO directions. **(T-1)**.

2.13.7. Ensure stakeholders are identified that may be affected by the implementation and operation of the IT. **(T-2)**.

2.13.8. Ensure the IT has a designated Information System Security Manager (ISSM) with the support, authority, and resources to satisfy established responsibilities for managing the IT's cybersecurity posture. **(T-1)**.

2.13.9. Plan and budget for all software assurance (SwA) activities (e.g. adopt SwA best practices, third party, secure coding standards, automated scans, etc…) during all phases of the software development lifecycle (SDLC). **(T-2)**.

2.13.10. In coordination with the Information Owner/Steward, decide who has access to the system (and with what types of privileges or access rights) and ensure system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). **(T-2)**.

2.13.11. Based on guidance from the SCA and AO, inform appropriate organizational officials of the need to conduct the full RMF assessment and authorization; ensure the necessary resources are available for the effort, and provides the required IT access, information, and documentation to the SCA. **(T-2)**.

2.13.12. Receive the security assessment results from the SCA and develop a POA&M for all identified weaknesses. **(T-1)**. After taking appropriate steps to reduce or eliminate weaknesses, the ISO will assemble the authorization package and submit the package to the SCA for assessment and subsequently to the AO for an authorization decision. **(T-1)**.

2.13.13. Ensure open POA&M items are closed on time. **(T-2)**.

2.13.14. Ensure consolidated A&A documentation is maintained for systems with instances at multiple locations. **(T-2)**.

2.13.15. Ensure, with the assistance of the ISSM, the system is deployed and operated according to the approved System Security Plan (SSP) and the authorization package (i.e., the AO's authorization decision). **(T-1)**.

2.13.16. Conduct specific duties outlined in the KS. **(T-2)**.

2.14. Program Manager (PM)/System Manager (SM). PM/SMs will:

2.14.1. Identify, implement, and ensure full integration of cybersecurity into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, operation, and sustainment IAW AFI 63-101, Acquisition and Sustainment Life Cycle Management, DoDI 8510.01 and AFMAN 33-210 for guidance. **(T-0)**.

2.14.2. Plan and coordinate for all IT cybersecurity requirements IAW applicable guidance**. (T-2)**.

2.14.3. Ensure that ISs and PIT systems under their purview have cybersecurity-related positions assigned in accordance with AFMAN 33-285. **(T-2)**.

2.14.4. Assign an ISSM for the program office and ensure they have the proper certification IAW AFMAN 33-285. **(T-1)**.

2.14.5. Ensure the IS or PIT system is registered IAW AFI 33-141, AF IT Portfolio Management and Investment Review.

2.14.6. Develop and maintain a cybersecurity strategy as applicable and IAW AFMAN 33-407.

2.14.7. Ensure operational systems maintain a current ATO. **(T-1)**.

2.14.8. Ensure all changes are approved through a configuration management process, are assessed for cybersecurity impacts and reported to the SCA as applicable. **(T-2)**.

2.14.9. Track and implement the corrective actions identified in the POA&M in the Enterprise Mission Assurance Support Service (eMASS). **(T-0)**. POA&Ms provide visibility and status of security weaknesses to the ISO, Information Owner(s), AO and AF SISO.

2.14.10. Ensure annual and milestone security reviews are conducted and selected RMF controls are tested IAW this instruction, the CM plan and OMB Circular A-130, Management of Federal Information Resources ISO FISMA. **(T-0)**. The PM/SM will brief the results of both security reviews and the RMF control tests at the governance boards for the appropriate mission area in accordance with the board requirements. **(T-0)**.

2.14.11. Report security incidents to stakeholder organizations. **(T-2)**. The PM/SM will conduct root cause analysis for incidents and develop corrective action plans. **(T-2)**.

2.14.12. Ensure the program is resourced with individuals knowledgeable in security engineering and security technical assessments IAW AFMAN 33-285. **(T-2)**. These efforts support the SCA's assessment and the AO's authorization decision for IT that is subject to the RMF process IAW AFMAN 33-210.

2.14.13. In coordination with the Information Owner/Steward, ensure that a Privacy Impact Assessment is completed for IT that process and/or stores Personal Identifiable Information (PII). **(T-0)**.

2.15. Information System Security Manager (ISSM). The ISSM is the primary cybersecurity technical advisor to the AO for AF IT. For base enclaves, the ISSM manages the installation cybersecurity program, typically as a function of the Wing Cybersecurity Office. That program ISSM may also serve as system ISSM for the enclave and reports to the CS/CC as the PM for the base enclave. The ISSM will:

2.15.1. Act on behalf of the AO to maintain the authorization of the system throughout its lifecycle; therefore, if the ISSM is not qualified to serve, the AO or the AODR may request the PM/SM designate a suitable replacement. **(T-3)**.

2.15.2. Complete training and maintains cybersecurity certification IAW AFMAN 33-285 (Individuals in this position must be US citizens). **(T-0)**. Proof of training (e.g. certificate) is included as an artifact to the IS's or PIT systems A&A package.

2.15.3. Support the ISO on behalf of the AO in implementing the RMF. **(T-3)**.

2.15.4. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program.

2.16. Information System Security Officer (ISSO). The ISSO is responsible for ensuring the appropriate operational security posture is maintained for AF IT under their purview. This includes the following activities related to maintaining situational awareness and initiating actions to improve or restore cybersecurity posture. ISSOs (formerly system level IA Officers), or the ISSM if no ISSO is appointed, will:

2.16.1. Implement and enforce all AF cybersecurity policies, procedures, and countermeasures using the guidance within this instruction and applicable cybersecurity publications. **(T-1)**.

2.16.2. Complete and maintain required cybersecurity professional certification IAW AFMAN 33-285 (Individuals in this position must be US citizens). **(T-0)**.

2.16.3. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program.

2.17. Cybersecurity Liaison. Each organizational command or other cognizant authority (i.e., group commander, Wing Cybersecurity Office) must appoint a Cybersecurity Liaison (formerly Organizational IAO) when cybersecurity functions are consolidated to a central location or activity. **(T-1).** Additional (subordinate) cybersecurity liaison positions may be assigned for additional support at the discretion of organizations or based upon mission requirements, however, only one primary and one alternate cybersecurity liaison is mandatory. A cybersecurity liaison will:

2.17.1. Develop, implement, oversee, and maintain an organization cybersecurity program that identifies cybersecurity requirements, personnel, processes, and procedures. **(T-1)**.

2.17.2. Supervise the organization's cybersecurity program. **(T-2)**.

2.17.3. Implement and enforce all Air Force cybersecurity policies and procedures using the guidance within this instruction and applicable specialized (COMSEC, COMPUSEC, TEMPEST etc.) cybersecurity publications. **(T-1)**.

2.17.4. Assist the wing cybersecurity office in meeting their duties and responsibilities. **(T-3)**.

2.17.5. Ensure all users have the requisite security clearances, supervisory need-to-know authorization, and are aware of their cybersecurity (via cybersecurity training) before being granted access to Air Force IT according to AFMAN 33-282, chapter 4, AFI 31-501 and AFMAN 33-152. **(T-1)**.

2.17.6. Ensure all users receive cybersecurity refresher training on an annual basis. **(T-2)**.

2.17.7. Ensure IT is acquired, documented, operated, used, maintained, and disposed of properly and in accordance with the IT's security A&A documentation as prescribed by AFMAN 33-210. **(T-1)**.

2.17.8. Ensure proper CM procedures are followed. **(T-1)**. Prior to implementation and contingent upon necessary approval according to this instruction and AFMAN 33-210, the cybersecurity liaison will coordinate any changes or modifications to hardware, software, or firmware with the wing cybersecurity office and system-level ISSM or ISSO. **(T-1)**.

2.17.9. Report cybersecurity incidents or vulnerabilities to the wing cybersecurity office. **(T-3)**.

2.17.10. In coordination with the wing cybersecurity office, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered. **(T-3)**.

2.17.11. Implement and maintain required cybersecurity (COMSEC, COMPUSEC and TEMPEST) countermeasures and compliance measures IAW AFI 10-712, Telecommunications Monitoring and Assessment Program (TMAP). **(T-1)**.

2.17.12. Initiate requests for temporary and permanent exceptions, deviations, or waivers to cybersecurity requirements or criteria according to this instruction and applicable specialized cybersecurity publications. **(T-1)**.

2.17.13. When called upon to assist with an assessment conducted by the DIB CS/Cybersecurity program office, provide subject matter experts to analyze the data and provide recommendations for further action. **(T-3)**.

2.17.14. Maintain all IS authorized user access control documentation IAW the applicable Air Force records Information Management System (AFRIMS). **(T-3)**.

2.18. Information Systems Security Engineer (ISSE). The ISSE is any individual, group, or organization responsible for conducting information system security engineering activities. Reference NIST SP 800-37, *Applying the Risk Management Framework to Federal Information Systems*, for additional details.

2.18.1. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration.

2.18.2. Information system security engineers are an integral part of the development team (e.g., integrated project team) designing and developing organizational information systems or upgrading legacy systems.

2.18.3. Information system security engineers employ best practices when implementing security controls within an information system including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.

2.18.4. System security engineers coordinate their security-related activities with information security architects, senior information security officers, information system owners, common control providers, and information system security officers.

2.18.5. IAW DoD 8570.01-M, Personnel performing any IA Workforce System Architecture and Engineering (IASAE) specialty function(s) (one or more functions) at any level must be certified to the highest level function(s) performed. **(T-0)**.

2.19. Information Owner/Steward. An organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal as defined in CNSSI 4009, National Information Assurance Glossary. The Information Owner/Steward will:

2.19.1. Plan and budget for security control implementation, assessment, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management. **(T-2)**.

2.19.2. Establish the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retain that responsibility even when the information is shared with or provided to other organizations. **(T-1)**.

2.19.3. Provide input to ISOs on the security controls selection and on the derived security requirements for the systems where the information is processed, stored, or transmitted. (A single IS may contain information from multiple information owners/stewards.) **(T-1)**.

2.19.4. Where a single IS may contain information from multiple information owners/stewards, provide input to ISO for the IS regarding security controls selection and derived security requirements for the systems where the information is processed, stored, or transmitted. **(T-1)**.

2.19.5. Thoroughly review the assessment and then releases the authorization package to the AO, thereby indicating to the AO that the system's cybersecurity posture satisfactorily supports mission, business, and budgetary needs (i.e., indicates the mission risk is acceptable); enabling the AO to balance mission risk with community risk in an authorization decision. **(T-1)**.

2.19.6. Maintain statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. **(T-0)**.

2.20. Headquarters Air Force Space Command (HQ AFSPC). As Lead Command for all Air Force Cyberspace Operations via the 24AF(AFCYBER), AFSPC is the Air Force focal point for establishment, operation, maintenance, defense, exploitation, and attack Cyberspace Operations. AFSPC coordinates the prioritization of all Cyberspace Infrastructure requirements. AFSPC will:

2.20.1. Cyber orders issued by AFSPC/CC or his/her delegated representative are military orders issued by order of the Secretary of the Air Force.

2.20.2. Support PEOs and PMs in the research, development, test and evaluation, and sustainment of cybersecurity or cybersecurity-enabled capabilities of AF space systems and products in consultation with the other MAJCOMs.

2.20.3. Develop and sustain processes for rapid cybersecurity capability insertion to address new or rapidly developing threats to the AFIN.

2.20.4. Ensure space PEOs and PMs/ISOs comply with cybersecurity requirements outlined in DoDI 8580.1, DoDI 8581.01, this instruction, and AFMAN 33-210.

2.20.5. Establish cybersecurity education and training for space PEOs and PMs/ISOs according to the requirements outlined in AFMAN 33-285.

2.20.6. Manage and advise the CDS program for space systems.

2.20.7. Manage the AF Cryptologic Modernization Program and oversees the AF COMSEC Office of Record (CoR) for COMSEC IAW AFMAN 33-283.

2.20.8. Coordinate all cryptographic equipment requests to reduce duplication of effort and ensure sustainability.

2.20.9. Manage all requests for support from NSA for cryptographic equipment certification, coordinate validation, and recommend prioritization for the AF SISO

2.20.10. Perform responsibilities IAW AFMAN 33-286, Air Force TEMPEST Program. This includes developing/managing necessary forms to include the AF Form 4170, Emission Security Assessments/Emission Security Countermeasures Review. AFSPC will executes the TEMPEST program and coordinates with the AF CTTA, as outlined in AFSSI 7700 (to become AFMAN 33-286).

2.20.11. Establish and maintain Method and Procedure Technical Orders (MPTOs) associated with cybersecurity policies.

2.20.12. Implement the AF cybersecurity workforce certification and training program according to DoDD 8570.01, DoD 8570.01-M, and AFMAN 33-285.

2.20.13. Review, evaluate, and interpret AF cybersecurity doctrine, policy, and procedures. AFSPC will make recommendations on implementation of the doctrine, policy, and procedures to SAF/CIO A6.

2.20.14. Develop, coordinate, promulgate, and maintain AF (component-level) cybersecurity control specifications applicable to ISs residing on or connecting to the AFIN, if required.

2.20.15. Provide guidance and support to cybersecurity offices in developing, implementing, and managing their cybersecurity programs.

2.20.16. Establish a Cross Domain Solution Office (CDSO) to manage the AF CDS program.

2.20.17. Advocate issues from customers with Air Staff and the CDS Secret Internet Protocol Router Network Connection Approval Office at DISA.

2.20.18. Serve as the AF focal point for coalition networking issues specific to the command, control, communications and computers infrastructure, core e-mail, file sharing, print, collaboration tools, video teleconferencing (VTC), and web browsing capabilities. AFSPC will coordinate with focal points of other functional communities (AF/A2, etc.) on coalition networking issues for other infrastructures (intelligence, surveillance, and reconnaissance, etc.).

2.20.19. Provide the following to SAF CIO/A6 and the SISO:

2.20.19.1. Situational awareness (SA) report on the operational status and network health of the globally interconnected, end-to-end set of AF unique information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), mission, SPO and PMO managed systems and enclaves, data, and security.

2.20.19.2. SA report related to outage and other network events impacting the AFIN or the supported Combatant Command (COCOM) mission.

2.20.19.3. SA report on completion of cyber orders or inability to complete assigned tasks.

2.20.19.4. Tasks specified above do not replace any requirement for OPREP reporting outlined in AFI 10-206.

2.20.20. Manage the AF PPS program and procedures according to this instruction, DoDI 8551.01, and USCYBERCOM orders. Advocate issues from customers with AF/A3C/A6C Staff and the DoD PPS Program Manager at DISA.

2.20.21. Advocate issues from AF activities with DoD PPS Management.

2.20.22. Provide guidance and support regarding PPS policy and procedures.

2.20.23. Serve as the primary with one or more alternate AF representatives to the DoD PPS TAG according to DoD guidance.

2.20.24. Serve as the primary POC with one or more alternates to register (aka declare) and maintain PPS for AF ISs in the DoD PPS central Registry according to DoD 8551.01.

2.20.25. Support and manage the AF PKI Systems Program Office (PKI SPO) to manage AF identity credentials for human and non-person entities. AFSPC will provide guidance and support to that office in the implementation and management of PKI and other IdAM capabilities to support Air Force operational and mission needs.

2.20.26. Process requested for PPS exceptions, deviations, or waivers according to this instruction and DoD policy and guidance (e.g. DoD 8551.01, USCYBERCOM orders, PPSM Exception Management Process).

2.20.27. Execute the AF COMSEC program and perform COMSEC responsibilities IAW AFMAN 33-283, Communications Security (COMSEC) Operations.

2.20.28. Perform responsibilities IAW AFMAN 33-286. This includes developing/managing necessary forms to include AF Form 4170, Emission Security Assessments/Emission Security Countermeasures Reviews.

2.21. MAJCOM Cybersecurity Office or Function will:

2.21.1. Support the principles of availability, integrity, confidentiality, authentication, and non-repudiation of information and information systems for the purpose of protecting and defending the operation and management of Air Force IT and National Security System (NSS) assets and operations.

2.21.2. Develop implement, oversee, and maintain a MAJCOM cybersecurity program that identifies cybersecurity architecture; requirements; objectives and policies; personnel; and processes and procedures.

2.21.3. Ensure cybersecurity workforce is identified, trained, certified, qualified, tracked, and managed IAW DoD and AF cybersecurity Workforce Improvement Program (WIP) directives and policies such as DoDD 8570.01, DoD 8570.01-M, AFMAN 33-210 and AFMAN 33-285. NOTE: If the individual is performing only COMSEC management duties, DoD 8570.01-M does not require the individual to be certified under this program.

2.21.4. Report the status of their cybersecurity workforce (civilian, military, and contractors) qualifications to the SAF/CIO A6 IAW Paragraph 7.2.of AFMAN 33-285.

2.21.5. Ensure that AF PKI Local Registration Authorities (LRAs) are established and maintained at all MAJCOM bases

2.21.6. Serve as a member of any appropriate Configuration Control Boards (CCB) or steering groups to address MAJCOM cybersecurity program issues.

2.21.7. Coordinate Inspector General (IG) inspections and associated responsibilities according to and AFI 90-201.

2.21.8. Review AF Form 4169 exception/waiver submissions, as appropriate, to maintain situational awareness

2.21.9. Ensure proper identification of manpower and personnel assigned to cybersecurity functions. MAJCOM Cybersecurity Office/Function will ensure this information is entered and maintained in the appropriate Air Force personnel databases.

2.21.10. IAW AFI 10-712, maintain organizational e-mail account with an SMTP alias of <MAJCOM>**.cybersecurity@us.af.mil**

2.22. Wing Cybersecurity Office (WCO). Develops and maintains the wing cybersecurity program. The wing cybersecurity office addresses all cybersecurity requirements on the base for IT under the control of the base Communications Squadron/Flight, including IT of tenant units (i.e., FOAs, DRUs, and other service units) unless formal agreements exist. NOTE: For bases

with more than one wing, the designated host wing is responsible to provide this function. For Joint bases, the AF is responsible for all AF-owned IT and infrastructure. The WCO will:

2.22.1. IAW AFMAN 33-285, track and manage cybersecurity positions assigned by a commander which includes: system ISSMs/ISSOs assigned by PM's, COMSEC Account Managers (CAMs), COMSEC Responsible Officers (CROs), Cybersecurity Liaisons, Privileged Users, and Secure Voice Responsible Officers (SVROs).

2.22.2. Assign trained cybersecurity personnel IAW DoD requirements for IAM Level I or Level II categories and ensure certifications are also maintained IAW DoD requirements. **(T-0)**. ***NOTE:*** If the individual is performing only COMSEC management duties, refer to AFMAN 33-285 for position specific certifications.

2.22.3. Manage the overall COMSEC posture of their installation. The WCO will appoint one primary and at least one alternate COMSEC manager to oversee the wing COMSEC program and to assist and advise them in COMSEC matters IAW AFMAN 33-283, COMSEC Operations. **(T-0)**. The wing commander may delegate appointment authority to the unit commander of the supporting COMSEC account.

2.22.4. Establish COMPUSEC in the host wing cybersecurity office. **(T-1).** The cybersecurity office addresses all COMPUSEC requirements on the base, including those of tenant units (i.e. FOAs, DRUs, and other MAJCOM units) unless formal agreements exist.

2.22.5. Establish TEMPEST in the host wing cybersecurity office. **(T-1).** The cybersecurity office addresses all TEMPEST requirements on the base, including those of tenant units (i.e. FOAs, DRUs, and other MAJCOM units) unless there are other formal agreements.

2.22.6. Manage the Identity Management Program (PKI, Common Access Card (CAC), Air Force Directory Service (AFDS) Programs) IAW AFMAN 33-282.

2.22.7. Assist all base organizations and tenants in the development and management of their cybersecurity program. **(T-1).**

2.22.8. Designate a base enclave ISSM (for organization-level cybersecurity program) to develop, implement, oversee, and maintain the installation cybersecurity program. **(T-1).**

2.22.9. Provide oversight and direction to Cybersecurity Liaison (for organizational level programs) according to this instruction, AFI 33-115 and specialized cybersecurity publications. **(T-1)**. Specific responsibilities include but are not limited to the below items. The WCO will:

2.22.9.1. Ensure Cybersecurity Liaison receives proper cybersecurity training. **(T-1).**

2.22.9.2. Ensure Cybersecurity Liaisons are aware of and follow cybersecurity policy and procedures. **(T-1).**

2.22.9.3. Ensure Cybersecurity Liaison s review weekly alerts, bulletins, and advisories impacting security of an organization's cybersecurity program. **(T-1).**

2.22.10. Ensure cybersecurity guidance, and standard operating procedures (SOP) are prepared, maintained, and implemented by each unit. **(T-3).**

2.22.11. Monitor implementation of cybersecurity guidance and ensure appropriate actions to remedy cybersecurity deficiencies. **(T-3).**

2.22.12. Ensure cybersecurity inspections, tests, and reviews are coordinated. **(T-3)**.

2.22.13. Ensure all cybersecurity management review items are tracked and reported. **(T-3)**.

2.22.14. Report security violations and incidents to the AO and Air Force network operations activities according to AFI 33-115, Air Force Information Technology (IT) Service Management) and CJCSM 6510.01B, Cyber Incident Handling Program. **(T-1)**.

2.22.15. Ensure cybersecurity incidents are properly reported to the AO and the Air Force network operations reporting chain, as required, and that responses to cybersecurity related alerts are coordinated; all according to the requirements of AFI priveleged115. **(T-1).**

2.22.16. Ensure software management procedures are developed and implemented according to configuration management (CM) policies and practices for authorizing use of software on ISs. **(T-1).**

2.22.17. Serve as member of the base-level CM board or delegates this responsibility to an appropriate Action Officer. **(T-3).**

2.22.18. Maintain organizational e-mail account with an SMTP alias of <wing>**.cybersecurity@us.af.mil.** **(T-3).**

2.23. Organizational Commander. Commander will assign one Cybersecurity Liaison and at least one alternate to execute cybersecurity responsibilities protecting and defending information systems by ensuring the availability, integrity, confidentiality, authentication, and non-repudiation of data through the application of cybersecurity measures outlined herein. **(T-1).** Commanders or equivalent at all levels will maintain these responsibilities through the following programs:

2.23.1. Computer Security (COMPUSEC) Program IAW AFMAN 33-282.

2.23.2. Communications Security (COMSEC) Program IAW AFMAN 33-283.

2.23.3. TEMPEST Program Management IAW AFMAN 33-286. TEMPEST: A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

2.23.4. On-Hook Telephone Security Program. **(T-1)**. Organization commanders will ensure their program meets the following:

2.23.4.1. Ensure the number of telephones used is the minimum necessary to meet operational requirements. **(T-3)**.

2.23.4.2. Apply appropriate telephone security measures in discussion areas and ensure adequate protection for classified or sensitive discussions IAW National telephone Security Working group (NTSWG) publications. **(T-3)**.

2.23.4.3. Use physical security safeguards to prevent unauthorized personnel from obtaining clandestine physical access to the telephone system or components of the system. **(T-3)**.

2.24. Privileged User with cybersecurity responsibilities (e. g. Functional System Administrator). NOTE: Enterprise Information System (EIS) content managers and site designers (e.g. Microsoft SharePoint Site Owners, AF Portal Content Managers) who don't have administrative privileges to the overall IS are not considered Privileged Users. Additionally,

AFMAN 33-285 and AFI 33-115 identify those individuals with certain elevated rights who are not considered Privileged users. Privileged users will:

2.24.1. Complete training and maintains certification IAW AFMAN 33-285.

2.24.2. Configure and operate IS according to cybersecurity policies and procedures and notify the AO, ISSM or ISSO of any changes that might adversely impact cybersecurity. **(T-1).**

2.24.3. Ensure IT under their management is properly patched per guidance from the PEO. **(T-3).**

2.24.4. Conduct and document annual cybersecurity inspection of their IT per the guidance provided the IT PEO. **(T-3).** Provides report to WCO annually.

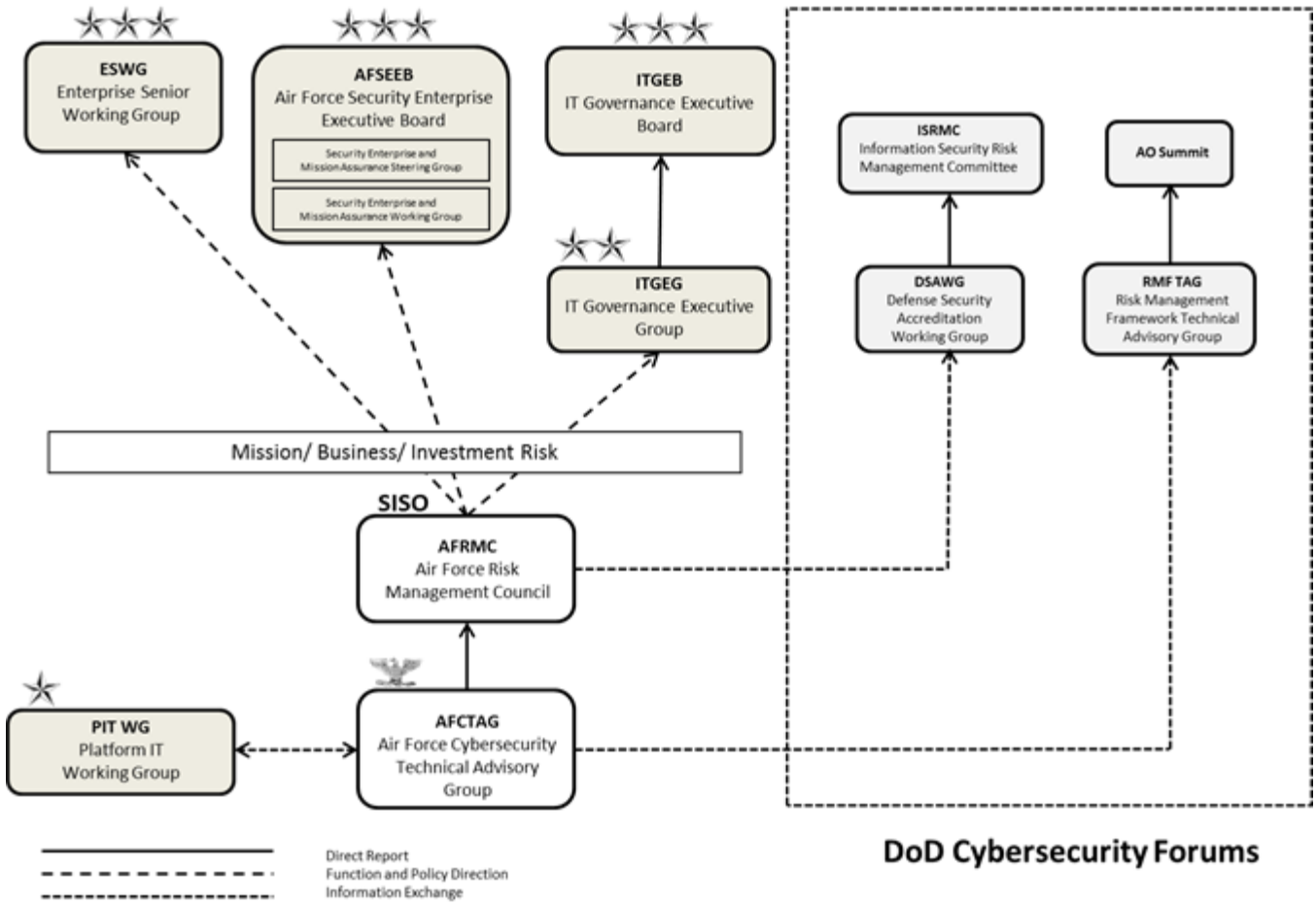
2.24.5. Establish and manage authorized user accounts for ISs, including configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed. **(T-3).**

Chapter 3

CYBERSECURITY GOVERNANCE

3.1. Cybersecurity Governance. Cybersecurity governance occurs at all levels of the Air Force enterprise and ensures cybersecurity strategies are aligned with mission and business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility. The Air Force Cybersecurity Governance Structure (Figure 3.1) formalizes how the AF manages cybersecurity risk with respect to the existing Air Force and DoD corporate boards and processes. The intention is to ensure cybersecurity is addressed in the appropriate forums for both mission/business risk and IT investment/portfolio management. Current governance forums do not regularly discuss cybersecurity nor the risk management process on a regular basis. These new forums ensure these topics are raised to the appropriate level and informed decisions can be made.

Figure 3.1. Air Force Cybersecurity Governance.



3.2. Governance Process. The governance process ensures compliance with Title 44 United States Code (USC) § 3541, Federal Information System Management Act of 2002 (FISMA), requiring senior agency officials to provide security for information and ISs that support the operations and assets under their control.

3.3. Governance Bodies. The Air Force leverages existing Air Force and DoD governance bodies (shaded areas of Figure 3.1—AFSEEB, ITGEB, ITGEG, ESWG, etc.) to discuss cybersecurity risk topics and make organizational and mission/business area risk decisions. This instruction does not define the scope or responsibilities of these existing bodies. The following governance groups provide focused management and oversight of the Air Force Cybersecurity Program. Charters and process guides for each of these organizations are in development.

3.4. Air Force Risk Management Council (AFRMC). The AFRMC provides a forum for the senior cybersecurity professionals to validate and vet issues concerning cybersecurity risk from a mission and business perspective. The council reviews proposed Mission Area or DoD Component RMF control overlays, A&A guidance, and additional AF controls for compatibility with baseline controls and with other established control sets. They standardize the cybersecurity implementation processes for both the acquisition and lifecycle operations of Air Force Information Technology and Cyberspace systems. They advise and make recommendations as needed to existing governance bodies. Finally, they adjudicate assignment of Air Force Information Technology and Cyberspace systems to the appropriate Authorizing Official for those systems which fall outside of the defined authorization boundaries.

3.4.1. Chaired by the AF Senior Information Security Officer (AF SISO)

3.4.2. Attendees include all Air Force Security Control Assessors, 24 AF/A3, 624 OC, and SAF/CIO A6C Mission Area Integrators (MAI)

3.4.3. Monthly VTC or SIPR Defense Collaboration Services (DCS) with an annual in-person meeting

3.5. AF Cybersecurity Technical Advisory Group (AFCTAG). The AFCTAG provides technical cybersecurity subject matter experts (SMEs) from across the MAJCOMs and functional communities to facilitate the management, oversight, and execution of the AF Cybersecurity Program. The TAG examines cybersecurity related issues common across Air Force entities and provide recommendations to the AF SISO and DSWAG on changes to the baseline security controls or configurations.

3.5.1. Co-chaired by the SAF/CIO A6S Cybersecurity Division Chief and AFSPC/A6S Division Chief

3.5.2. Attendees include all MAJCOM and functional cybersecurity subject matter experts

3.5.3. Quarterly DCS

3.6. AF AO Summit. The AO Summit is not a governance body but rather an enabler for both an enterprise-wide and converged organizational perspective to cybersecurity policy development, oversight, implementation, and training. This venue provides the CIO and Authorizing Officials an opportunity to discuss issues relevant and significant to AOs and their SCAs and develop recommended a way-forward for use by the Department.

3.6.1. Chaired by SAF CIO/A6

3.6.2. Attendees include all Air Force Authorizing Officials, Mission Area Owners (MAO), 24 AF/CC, and AF SISO

3.6.3. Quarterly VTC with an annual in-person meeting

Chapter 4

CYBERSECURITY IMPLEMENTATION

4.1. Air Force Cybersecurity Program. The AF Cybersecurity Program synchronizes and standardizes the cybersecurity requirements of AF IT.

4.1.1. Cybersecurity is integrated into all aspects of the AF Enterprise Architecture according to AFI 33-401.

4.1.2. Cybersecurity professionals coordinate cybersecurity projects across multiple investments through Portfolio Management according to AFI 33-141, Air Force Information Technology Portfolio Management and Investment Review.

4.1.3. All elements of an IT cybersecurity program are developed, documented, implemented, and maintained through the AF A&A program. Please reference AFMAN 33-210 for further information.

4.1.4. Cybersecurity professionals adhere to CJCSI 6510.01F and AFI 33-115 on use of DoD-provided, enterprise-wide automated tools/solutions (e.g., Host Based Security System (HBSS)) to ensure interoperability with DoD- and AF- provided enterprise-wide solutions for remediation of vulnerabilities for endpoint devices.

4.1.5. ISSMs and ISSOs protect ISs, their operating system, peripherals (media and devices), applications, and the information it contains against loss, misuse, unauthorized access, or modification. Ensure compliance with AFMAN 33-282 and MPTO 00-33B-5006, End-point Security for Information Systems. These procedures ensure the computing environment complements the AF IS cybersecurity program. MPTO 00-33B-5006 provides standard procedures derived from cybersecurity controls and other measures for organizations to maintain the confidentiality, integrity, and availability of any AF IS cybersecurity program

4.1.6. All authorized users ensure protection of all ISs against tampering, theft, and loss. Protect ISs from insider and outsider threats by controlling physical access to the facilities and data by implementing procedures identified in Joint, DoD, AF publications, and organizationally created procedures. Basic end point security procedures are located in MPTO 00-33B-5006.

4.2. Cybersecurity Workforce Training and Certification. This instruction and supporting cybersecurity specialized publications standardize the naming conventions and functions of AF organizational (management) and IT level (technical or system-level) Cybersecurity personnel. These documents also prescribe training and certification requirements according to national and DoD policy consistent with and supplementary to the guidance outlined in AFMAN 33-285, Information Assurance (Cybersecurity) Workforce Improvement Program.

4.3. Information Assurance Workforce System Architecture and Engineering. IAW DoD 85701-M and AFMAN 33-285, personnel required to perform any IA Workforce System Architecture and Engineering (IASAE) specialty functions (one or more functions) at any level must be certified to the highest level functions(s) performed. **(T-1)**.

4.3.1. Cybersecurity privileged user or management functions, see AFMAN 33-285.

4.3.2. AO and other A&A training requirements, see AFMAN 33-285.

4.3.3. COMPUSEC training and requirements, see AFMAN 33-282

4.3.4. COMSEC training requirements follow guidance in AFMAN 33-283

4.3.5. TEMPEST training requirements, see AFMAN 33-286.

4.4. Cybersecurity Inspections. Cybersecurity disciplines are assessed under the Air Force Inspection System (AFIS) IAW AFI 90-201 and through self-assessments communicators (SACs) located in MICT.

4.4.1. Inspectors/auditors perform inspections according to guidance in this instruction and applicable AF Cybersecurity publications for COMSEC, COMPUSEC, and TEMPEST (Formerly known as EMSEC).

4.4.2. ISOs comply with formal testing and certification activities according to AFI33-210.

4.4.3. Inspect or assess performance measures and metrics based on enterprise-wide (and individual elements where appropriate) cybersecurity performance and assess cybersecurity trends. Limit the measurements and metrics to Federal and DoD Cybersecurity reporting requirements.

4.4.4. Inspect AF PKI Local Registration Authorities (LRAs) in accordance with AFMAN 33-282 and associated MICT section.

4.5. Notice and Consent Monitoring and Certification. All AF installations, AF organizations on joint bases, circuits, and ISs must comply with DoD notice and consent certification requirements for monitoring to occur by authorized activities as well as comply with installation certification procedures IAW AFI 10-712, Telecommunications Monitoring and Assessment Program (TMAP) (to become Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process). **(T-0)**.

4.6. Connection Management.

4.6.1. AF activities must adhere to the DISA Connection Approval Process if the system is connected to the Non-Secure Internet Protocol Router Network (NIPRNET) or Secure Internet Protocol Router Network (SIPRNET). **(T-0).** Connection Approval Process information can be found at **http://www.disa.mil/connect**. For all AF ISs accessing the DISN, get appropriate service (e.g., DISA) coordination and authorization before proceeding with combatant command coordination and/or Joint Staff approval.

4.6.2. AF activities comply with AFMAN 33-210 for connection approval to the Air Force Information Networks (AFIN).

4.6.3. AF A6S provides AF representation to the DSAWG. The DSAWG represents the DISN community and advises the DISN AOs of community acceptance or rejection of risk. DISN connection decisions rest with the DISN AOs. AF A6S work with AF activities involved in the adjudication of conflicts related to DISN connection decisions.

4.7. Commercial Internet Service Providers (ISPs). The only DoD authorized access to the Internet is via a NIPRNET connection.

4.7.1. Organizations requiring a connection (wired or wireless) to the Internet via a fixed Commercial ISP solution must accredit the system and submit an AF Form 4169, Request for Waiver from Cybersecurity Criteria, through their WCO through AFSPC's Cyberspace

Support Squadron (CYSS) to SAF CIO/A6SC, the AF representative to the DoDIN Waiver Panel (GWP) IAW CJCSI 6211.02D. **(T-2)**. Use AF Form 4169 to document the request and prepare a DoDIN waiver brief in accordance with the DISA, "DISN Connection Process Guide" (**http://www.disa.mil/connect/waivers**). This applies to all Commercial ISP connection requests IAW AFI 33-115.

4.7.2. Use of mobile air cards and/or mobile hotspots for Temporary Duty (TDY)/mobile usage does not require a Commercial ISP waiver. Obtain approved devices and mobile data service through IT Commodity Council (ITCC) approved contracts. Use of these devices and services is not to be permanent. Configure all mobile hotspots and devices to applicable DISA Wireless STIGs. Use only approved encryption solutions (e.g. Cisco VPN Client, Juniper Network Connect, Citrix). Refer to DISA STIGs for use of mobile hotspot feature on Commercial Mobile Devices (CMDs)/smartphones. Organizations that use DoD devices that attach to the NIPR via these means must ensure they connect through a VPN first. **(T-2)**. Any other configuration is unauthorized.

4.8. Cross-Domain Solutions (CDS). Cross Domain Solutions (CDS). A CDS is a form of controlled interface providing the ability to manually and/or automatically access and/or transfer information between different security domains (e.g., between unclassified and classified). A CDS requires an additional approval process and authorization, separate from the review and approval for the Authorization to Connect (ATC) for the Command Communications Service Designator (CCSD). Developers and users refer to the CDS guidance, use only CDS-approved devices evaluated and validated through Certification Test and Evaluation or have a sufficient body of evidence to allow the Air Force Cross Domain Support Element (AF CDSE) to conduct a thorough risk analysis and adhere to CDS configuration guidelines. The purpose of and approval procedures for CDS are extracted from DoD, DISA, NSA, and the Unified Cross Domain Systems Management Office (UCDSMO) policies and guidance. For guidance on the most current CDS process, contact the AF CDSE, consult DoDI 8540.01, Cross Domain (CD) Policy, or visit the DISA Mission Partners website at **http://disa.mil/Services/Network-Services/Enterprise-Connections/Mission-Partner-Training-Program**.

4.8.1. Send all requests for CDSs and coalition information sharing solutions to AF CDSE at **nac.csni@us.af.mil** (**https://intelshare.intelink.gov/sites/afcdse/SitePages/Home.aspx**). This office provides the most current guidance for the CDS approval process..

4.8.2. The UCDSMO maintains a baseline list of NSA-certified solutions available for reuse contingent on approval by the DSAWG (available on SIPRNet at **https://intelshare.intelink.sgov.gov/sites/ucdsmo/default1.aspx**)

4.9. Security Configuration Management and Implementation. The ISSO (or designee) will comply with the following:

4.9.1. Securely configure and implement all IT products. **(T-1).** Cybersecurity reference documents, such as NIST SPs, DISA STIGs (**http://iase.disa.mil/stigs/**),NSA Security Configuration Guides, and other relevant publications are used as security configuration and implementation guidance. ISSOs will apply these reference documents according to this policy and AFMAN 33-210 to establish and maintain a minimum baseline security configuration and posture. **(T-1)**.

4.9.2. Review all changes to the configuration of IT (i.e., the introduction of new IT, changes in the capability of existing IT, changes to the infrastructure, procedural changes, or changes in the authorized or privileged user base, etc.) for cybersecurity impact prior to implementation. **(T-2)**. Document all configuration management and security requirements in the IT A&A package according to AFMAN 33-210 and CJCSI 6510_01F. **(T-0)**.

4.9.3. NIST Cryptographic Module Validation Program (CMVP) for Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, validation. **(T-0)**: **http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm**

4.9.4. Leverage and update DISA Approved Products List Integrated Tracking System (APLITS). **https://aplits.disa.mil/ (T-1)**

4.10. IT Acquisitions and Procurement. All acquisition and cybersecurity personnel must ensure cybersecurity is implemented in all IT acquisitions at levels appropriate to the system characteristics and requirements throughout the acquisition life cycle, according to AFI 63-101 and AFMAN 33-153.

4.10.1. All acquisition and cybersecurity personnel must ensure all IT hardware, firmware, and software components or products incorporated into DoDIN comply with evaluation and validation requirements in DoDI 8500.01 and CNSSP 11. **(T-1)**. Refer to CNSSP No. 11 for the latest process and policy guidance on this subject. Limit products to those listed on any of the lists below:

4.10.1.1. NSA-certified "TEMPEST" products: **https://www.nsa.gov/applications/ia/tempest/tempestPOCsCertified.cfm**

4.10.1.2. Common Criteria Evaluation and Validation Scheme (CCEVS): **http://www.commoncriteriaportal.org/products** and **http://www.niap-ccevs.org**

4.10.1.3. DoD Unified Capabilities Approve Products List (UC APL): **https://aplits.disa.mil/**

4.10.1.4. AF Evaluated Products List (AF EPL) **https://cs.eis.af.mil/afdaa/Lists/COTSGOTS%20Software/EPL.aspx**

4.10.1.5. Product Director Automated Movement and Identification Solutions ((PDAMIS) @**http://www.pdamis.army.mil**

4.10.2. Cybersecurity and Cybersecurity-enabled products are documented within the IS A&A package according to AFMAN 33-210.

4.10.3. WCOs, ISSOs, and ISSMs must ensure the procurement activities of all IT hardware, cellular, and peripheral devices (e.g., desktops, laptops, servers, BlackBerry® devices, tablets, cell phones, printers, scanners) follow the guidance in AFMAN 33-153, and the AF ITCC guidance available on the AF Portal. **(T-2)**.

4.10.4. WCOs, ISSOs, and ISSMs must ensure the procurement of telephone/voice switches is coordinated with Air Force Office of Special Investigations (AFOSI) for Technical Surveillance Countermeasures (TSCM) program. **(T-1)**.

4.10.5. IAW AFI 71-101, Volume 3, Air Force Technical Surveillance Countermeasure Program, the acquisition of voice systems require certification through the UC APL.

4.11. Air Force KMI. The Air Force Lifecycle Management Center (AFLCMC) manages the Air Force KMI program. KMI is the framework and services that provide the generation, production, storage, protection, distribution, control, tracking and destruction for all cryptographic keying material, symmetric keys as well as public keys and PKI certificates. The KMI system is comprised of nodes that provide the means to deliver cryptographic products, key management products and services to a large and diverse community of globally distributed users. ISOs and Cybersecurity professionals implement key management procedures according to AFMAN 33-283.

4.12. Public Key Infrastructure (PKI). The AF PKI SPO (AFLCMC/HNCYP) is responsible for the integration, implementation and sustainment of the DoD PKI, NSS PKI, AF PKIs, external federated PKIs and associated identity and access control management (ICAM) technologies to deny anonymity to our adversaries within the AF and associated COCOM systems. PKI authenticates users and systems on all AF networks via multiple, interoperable PKIs. PKI digital certificates provide both human identity credentials as well as non-person entity (NPE) identity credentials for all personnel, systems, services, devices, applications and data across all AF networks. ISOs and Cybersecurity professionals implement PKI, ICAM and Identity and Access Management (IdAM) procedures in accordance with AFMAN 33-282.PKI is implemented by AF ISOs and Cybersecurity professionals through the use of hardware tokens (CAC, AFNET-S token, Alternate Login Token (ALT), and Volunteer Logical Access Credential (VoLAC)) and software certificates on both AFNET and AFNET-S according to procedures in AFMAN 33-282.

4.13. System Security Engineering (SSE). Cybersecurity is to be integrated into the overall system acquisition and engineering process throughout the entire system life cycle via the information system's security engineering (SSE), according to DoDI 5134.16, *Deputy Assistant Secretary of Defense for Systems Engineering.*

4.14. COMPUSEC. The framework of the AF COMPUSEC IA program consists of a cyclic sequential security management model for risk management. This model is specific to information processed on AF computing systems and incorporates strategy, policy, awareness/training, implementation, assessment, remediation, and mitigation controls IAW AFMAN 33-283.

4.15. Communications Security. COMSEC refers to measures and controls taken to deny unauthorized persons information derived from ISs of the United States Government related to national security and to ensure the authenticity of such ISs. COMSEC protection results from applying security measures (i.e., crypto security, transmission security, etc.) to communications and ISs generating, handling, storing, processing, or using classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes applying physical security measures to COMSEC information or materials. Ensure all COMSEC activities comply with AFMAN 33-283 and associated AF Cybersecurity publications.

4.16. TEMPEST. TEMPEST denies interception and exploitation of classified, and in some instances unclassified, information by containing compromising emanations within a facility where information is being processed. Refer to AFMAN 33-286 for implementing countermeasures to protect against compromising emanations.

4.17. Operations Security (OPSEC). The OPSEC program is an operations function or activity and its goals are information superiority and optimal mission effectiveness. The emphasis is on OPERATIONS and the assurance of effective mission accomplishment. To ensure effective implementation across organizational and functional lines the organization's OPSEC Program Manager (PM), Signature Management Officer (SMO), or coordinator resides in the operations and/or plans element of an organization or report directly to the commander. For additional information see AFI 10-701, Operations Security (OPSEC).

4.18. Incident Response and Reporting. An incident is defined as an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an IS; or the information the IS processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security polices, security, procedures, or acceptable use policies (see CNSSI 4009).

4.18.1. For reportable cyber incidents (e.g., unauthorized access, denial of service, and malicious logic) in the AF network response hierarchy, refer to AFI 10-1701.

4.18.2. For any other service incident, which is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service, contact the applicable helpdesk.

4.18.3. For COMPUSEC incidents refer to AFMAN 33-282.

4.18.4. For COMSEC incidents refer to AFMAN 33-283.

4.19. Mobile Code. Comply with DoDI 8500.01 to protect ISs from the threat of malicious or improper use of mobile code during system acquisition and fielding. System developers and implementers follow guidelines in all applicable STIGs. Additional mobile code guidance is in AFMAN 33-282.

4.20. Ports, Protocols, and Services (PPS). The AF PPS Management Program provides policy and procedures on the use of PPS across the AFIN, consistent and complementary with the implementation of DoDI 8551.01, Ports, Protocols, and Service Management (PPSM), for additional PPS requirements, see AFSSI 8551, Ports, Protocols, and Services (PPSM) Management.

4.21. Physical Security. Access to and Physical Protection of Computing Facilities. Employ physical security measures (i.e., access control, visitor control, physical control, testing, etc.) for network and computing facilities that process publicly releasable, sensitive, or classified information to only authorized personnel with appropriate clearances and a need-to-know according to AFJI 31-102, Physical Security and DoD 5200.08-R, Physical Security Program.

4.22. Information Security. Comply with AFI 16-1404 for workplace security procedures and storage of documents and IT equipment.

4.23. Malicious Logic Protection. Protect AF IT from malicious logic (e.g., virus, worm, Trojan horse) attacks by applying a mix of human and technological preventative measures according to DoD 8500.01 and AFMAN 33-282. Continuous monitoring and patching of IS and PIT systems are mandated per AFMAN 33-210.

4.24. Data Encryption. Protect sensitive information; Controlled Unclassified Information (CUI); For Official Use Only (FOUO); Personally Identifiable Information (PII); Health Insurance Portability and Accountability Act (HIPAA); Privacy Act (PA); in transit and at rest with strong encryption, IAW DoD CIO Memorandum, and USCYBERCOM CTO 08-001,

Encryption of Sensitive Unclassified Data at Rest (DaR) on Mobile Computing Devices and Removable Storage Media Used Within the Department of Defense (DoD) and this instruction. For additional encryption requirements see, AFMAN 33-282.

4.25. Mobile Computing Devices. Mobile computing devices are IS devices such as Portable Electronic Devices (PEDs), laptops, and other handheld devices that can store data locally and authenticate to AF-managed networks through mobile access capabilities. Refer to AFMAN 33-282 for additional information on protections, deployment, use of Software Certificates and support of mobile computing devices.

4.26. Personal Activity Monitor (PAM) / Wearable Technology. Any non-stationary electronic apparatus with the capability of detecting, recording, storing, and or transmitting information about an individual's activity level, biological functions, or similar activities related to health and fitness. For additional information refer to AFMAN 33-282.

4.27. Wireless Services. WCOs, ISSOs, and ISSMs must ensure wireless services integrated or connected to AF ISs comply with DoDI 8500.01and DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG). **(T-0).** Refer to AFMAN 33-282 for additional information on protections, deployment and support of wireless services.

4.28. Non-Air Force IT utilized on AF installations.

4.28.1. Privately-owned Hardware and Software. Privately-owned hardware and software connected to the AFIN and used to process unclassified and/or unclassified sensitive information requires operational mission justification and AFIN AO approval. Document the approval between the user and government organization. The organizational ISSO maintains the documentation and provides it to the system ISSM as required. For additional information see AFMAN 33-282.

4.29. Peripheral Devices. A computer peripheral is any external device that provides input and output for the computer. Inputs devices transmit data and/or commands to a desktop or laptop (e.g. mouse, scanners, Smart boards, pointers, and keyboards). Output devices receive data from the desktop or laptop providing a display or printed product (e.g. monitors, printers, and multi-function devices (MFDs)). Refer to AFMAN 33-282 for additional information on the protections for peripheral devices.

4.30. Removable Media. Removable media is any type of storage media designed to be removed from a computer. This includes external hard drives, optical media (e.g., CDs, DVDs) and flash media (e.g., memory cards, USB flash drives, and solid-state drives). Refer to AFMAN 33-282 for additional information on removable media handling, configuration and use.

4.31. Collaborative Computing. Collaborative computing provides an opportunity for a group of individuals and/or organizations to share and relay information in such a way that cultivates team review and interaction in the accomplishment of duties and attainment of mission accomplishment. Configure and control collaborative computing technologies to prevent unauthorized users from seeing and/or hearing national security information and material at another user's workstation area. Establish safeguards to ensure the integration of data from various sources does not result in the creation of a higher classified data on ISs that are not rated to store or process at the higher level. Such instances are considered spillage and WCOs, ISSOs,

and ISSMs must address these. **(T-1)**. Refer to AFMAN 33-282 for additional information on collaborative computing and provisions on its deployment and use.

4.32. Spillage. This is when data is found on a system that has a lower security classification than that of the data. This term is also used when PII is found on a system that is not approved for processing, storing or transmitting of PII data. Refer to AFMAN 33-282, for additional information on spillage and incident reporting.

WILLIAM J. BENDER, Lt Gen, USAF
Chief of Information Dominance and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 100-235, *Computer Security Act of 1987*, January 8, 1988

Title 5 USC § 552a, *The Privacy Act of 1974, as amended* January 7, 2011

Title 10 USC § 2224, *Defense Information Assurance Program*, January 7, 2011

Title 44 USC § 3541, *Information Security (Federal Information System Management Act)*, December 17, 2002

Title 44 USC § 3602, *Office of Electronic Government*, December 17, 2002

OMB Circular A-130, *Management of Federal Information Resources*, November 28, 2000

ICD 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,* September 15, 2008

CNSSP 26, *National Policy on Reducing the Risk of Removable Media for National Security Systems*, November 2010

CNSSI 4009, *National Information Assurance (Cybersecurity) Glossary*, April 26, 2010

CNSSI 4031, *Cryptographic High Value Products*, 16 February 2012

NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Rev 1, February 2010

NIST 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011

NIST-SP 800-46, *Guide to Enterprise Telework and Remote Access Security*, April 2010

NIST-SP 800-88 Revision 1, *Guidelines for Media Sanitization, December 2014*

National Science and Technology Council Subcommittee on Biometrics Glossary, September 14, 2006

NSTISSAM TEMPEST/2-95A, *Red/Black Installation Guidance*, February 3, 2000

NSTISSI 4003, (FOUO) *Reporting and Evaluating COMSEC Incidents (U)*, December 2, 1991

CNSSI 4005, (FOUO) *Safeguarding Communications Security (COMSEC) Facilities and Materials,* August 22, 2011

CNSSI No. 4016, (FOUO) *National Information Assurance Training Standard For Risk Analysis*

CNSSI 4031, *Cryptographic High Value Products (CHVP)*, February 16, 2012

CNSSP 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, June 10, 2013

NSTISSP 200, *National Policy on Controlled Access Protection*, July 15, 1987

NSA/CSS Policy Manual 9-12, *NSA/CSS Storage Device Declassification Manual,* March 13, 2006

CJCSI 6211.02D, *Defense Information System Network (DISN) Responsibilities*, January 24, 2012

CJCSI 6510.01F, *Information Assurance (Cybersecurity) and Computer Network Defense (CND)*, February 9, 2011

CJCSM 6510.01B, *Cyber Incident Handling Program*, July 10, 2012

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, December 15, 2014

X.509 Certificate Policy for United States Department of Defense, February 9, 2005

FIPS140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001

DoDM 1000.13 v1, *DoD Identification (ID) Cards: ID Card Life-Cycle*, DoDI 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, DISA Security Technical Implementation Guides (STIGs), **http://iase.disa.mil/stigs/**

DoD Antivirus Solutions, **http://www.disa.mil/antivirus/index.html**

DoD Policy Memorandum, *Mobile Code Technologies Risk Category List Update*, March 14, 2011, **https://powhatan.iiie.disa.mil/mcp/mcpdocs.html**

DoD CIO Memorandum, *DoD Commercial Mobile Device Implementation Plan*, February 15, 2013

DoDI 4161.02, *Accountability and Management of Government Contract Property*, April 27, 2012

DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015

DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, February 24, 2012

DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Classified Information*, February 24, 2012

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, February 24, 2012

DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, February 24, 2012

DoDI 5200.02,*DoDPersonnel Security Program (PSP)*, March 21, 2014

DoDI 5200.08, *Security of DoD Installations and resources and the DoD Physical Security Review Board (PSRB)*, December 10, 2005

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, January 24, 2012

DoDI 3200.12, *DoD Scientific and Technical Information Program (STIP)*, August 22, 2013

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, June 16, 1992

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*, June 22, 2005

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, August 18, 1995

DoDD 5400.7, *DoD Freedom of Information Act (FOIA) Program*, July 28, 2011

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, February 10, 2009

DoDD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, April 14, 2004

DoDD 8500.01, *Cybersecurity*, March 14, 2014

DoDD 8521.01, *Department of Defense Biometrics*, February 21, 2008

DoDI 1035.01, *Telework Policy*, April 4, 2012

DoDI 1100.21, *Voluntary Services in the Department of Defense*, December 26, 2002

DoDI 5134.16, *Deputy Assistant Secretary of Defense for Systems Engineering* (DASD(SE)),” August 19, 2011

DoDI 5205.08, *Access to Classified Cryptographic Information*, November 8, 2007

DoDI 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/Cybersecurity) Activities*, January 29, 2010

DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*, November 3, 2009

DoDI 8510.01, *DoD Risk Management Framework (RMF)*, March 12, 2014

DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, May 24, 2011

DoDI 8520.03, *Identity Authentication for Information Systems*, May 13, 2011

DoDI O-8530.2, *Support to Computer Network Defense, (CND)*, March 9, 2001

DoDI 8540.01, *Cross Domain (CD) Policy*, May 8, 2015

DoDI 8550.01, *DoD Internet Services and Internet-based Capabilities*, September 11, 2012

DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*,May 28, 2014

DoDI 8580.1, *Information Assurance (Cybersecurity) in the Defense Acquisition System*, July 9, 2004

DoDI 8581.01, *Information Assurance (Cybersecurity) Policy for Space Systems Used by the Department of Defense*, June 8, 2010

DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*, June 6, 2012

USCYBERCOM Communications Tasking Orders (CTOs), **https://www.cybercom.mil/default.aspx**

AFPD 33-2, Information Assurance (Cybersecurity) Program, August 3, 2011

AFI 10-701, Operations Security (OPSEC), June 8, 2011

AFI 10-710, Information Operations Condition (INFOCON), August 10, 2006

AFI 10-712, Telecommunications Monitoring and Assessment Program (TMAP), June 8, 2011

AFI 16-107, Military Personnel Exchange Program, February 2, 2006

AFI 16-201, Air Force Foreign Disclosure and Technology Transfer Program, July 23, 2014

AFJI 31-102, *Physical Security*, May 31, 1991

AFI 31-401, Information Security Program Management, November 1, 2005

AFI 31-501, Personnel Security Program Management, January 27, 2005

AFI 31-601, Industrial Security Program Management, June 29, 2005

AFMAN 33-153, *Information Technology Asset Management (ITAM),* Mar 19, 2014

AFI 33-115, Information Technology Service Management

AFMAN 33-283, *Communications Security (COMSEC) Operations*, September 3, 2014

AFMAN 33-210, *Air Force Assessment and Authorization (A&A) Program (AFAAP), TBD),* December 23, 2008

AFI 33-332, Air Force Privacy and Civil Liberties Program, January 12, 2015

AFI 33-360, Publications and Forms Management, September 25, 2013

AFI 33-401, Air Force Architecting, May 17, 2011

AFI 36-2201, Air Force Training Program, September 15, 2010

AFI 36-3026_IP, Volume 1, Identification (ID) Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel, June 17, 2009

AFI 63-101/20-101, Integrated Life Cycle Management, March 7, 2013

AFI 71-101 Volume 3, The Air Force Technical Surveillance Countermeasures Program, January 16, 2013

AFI 90-201, The Air Force Inspection System, August 2, 2013

AFKAG-2L, (FOUO) *Air Force COMSEC Accounting Manual*, May 15, 2007

AFMAN 33-145, *Collaboration Services and Voice Systems Management,* September 6, 2012

AFMAN 33-152, *User Responsibilities and Guidance for Information Systems,* June 1, 2012

AFMAN 33-285, *Information Assurance (Cybersecurity) Workforce Improvement Program,* June 17, 2011

AFMAN 33-363, *Management of Records*, March 1, 2008

AFMAN 33-407, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, 24 October 2012*Air Force Records Information Management System Records Disposition Schedule (RDS)*

AFSPC/A6 Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133 Memorandum, July 6, 2011

624 OC TASKORD 2012-76-014, *Classified Message Incident (CMI) Declaration Authority & Handling Procedures*

MPTO 00-33A-1109, *Vulnerability Management*

MPTO 00-33B-5004, *Access Control for Information Systems*

MPTO 00-33B-5006, *End point Security for Information Systems*

MPTO 00-33B-5008, *Remanence Security for Information Systems*

MPTO 00-33D-2001, *Active Directory Naming Conventions*

T.O. 00-33A-1202-WA-1, *Air Force Network Account Management,* May 12, 2011

T.O. 31S5-4-7255-8-1, *Configuration and Operations Guide for Air Force Certificate-Based Smart Card Logon / Next Generation Using Personal Identity Verification (PIV) Certificate*

TO 31S5-4-7256-8-1, *Configuration and Operations Guide for Air Force Certificate-Based Smart Card Logon / Next Generation Using Alternate Security Identification (ALTSECID)*

Prescribed Forms:

AF Form 4167, Two-Person Control (TPC) COMSEC Material Inventory

AF Form 4170, Emission Security Assessments/Emission Security Countermeasures Reviews

Adopted Forms:

SF 312, Nondisclosure Agreement

SF 700, Security Container Information Form

DD Form 2875, System Authorization Access Request (SAAR)

DD Form 2946, DoD Telework Agreement

AF Form 4394, Air Force User Agreement Statement-Notice and Consent Provision

AF Form 847, Recommendation for Change of Publication

Abbreviations and Acronyms

AF —Air Force (as used in forms)

AF CTTA —Certified TEMPEST Technical Authority (CTTA)

AFCTAG -- AF —Cybersecurity Technical Advisory Group

AFI —Air Force Instruction

AFIA —Air Force Inspection Agency

AFIN —Air Force Information Networks

AFIS —Air Force Inspection Service

AFKAG —Air Force Cryptographic Aid, General

AFMAN —Air Force Manual

AFNET —The Air Force's underlying Non-Secure Internet Protocol Router Network (NIPRNet)

AFNET-S —The Air Force's underlying Secure Internet Protocol Router Network (SIPRNet)

AFNIC —Air Force Network Integration Center

AFOSI —Air Force Office of Special Investigations

AFPC —Air Force Personnel Center

AFPD —Air Force Policy Directive

AFRIMS —Air Force Records Information Management System

AFRMC —Air Force Risk Management Council

AFSC —Air Force Specialty Code

AFSPC —Air Force Space Command

AFSSI —Air Force Systems Security Instruction

ALT —Alternate Logon Token

ALTSECID —Alternate Security Identification

AIS —Automated Information System

AO —Authorizing Official

ATO —Authorization to Operate

A&A —Assessment & Authorization (formerly C&A)

C2 —Command and Control

CA —Certificate Authority

CAC —Common Access Card

CAM —COMSEC Account Manager

CAP —Cryptographic Access Program

CCB —Configuration Control Board

CCEVS —Common Criteria Evaluation and Validation Scheme

CDC —Cleared Defense Contractors

CDS —Cross-Domain Solutions

CDSE —Cross Domain Service Element

CDSO —Cross Domain Solution Office

CE —Computing Environment

CHVP —Cryptographic High Value Products

CI —Counterintelligence

CIA —Confidentiality, Integrity, Availability

CIO —Chief Information Officer

CITS —Combat Information Transport System

CJCSI —Chairman of the Joint Chiefs of Staff Instruction

CJCSM —Chairman of the Joint Chiefs of Staff Manual

CM —Configuration Management

CMI —Classified Message Incident

CMVP —Cryptographic Module Validation Program

CND —Computer Network Defense

CNSSI —Committee on National Security Systems Instruction

CNSSP —Committee on National Security Systems Policy

COCOM —Combatant Command

COI —Community of Interest

COMPUSEC —Computer Security

COMSEC —Communications Security

CoN —Certificate of Networthiness

CTO —Communications Tasking Order

CTS —Computerized Telephone Switch

CTTA —Certified TEMPEST Technical Authority

CUI —Controlled Unclassified Information

Cybersecurity —Information Assurance

CybersecurityAP —Cybersecurity Assessment and Assistance Program

CYSS —Cyberspace Support Squadron

DAMO —Damage Assessment Management Office

DaR —Data at Rest

DC3 —Department of Defense Cyber Crime Center

DCS —Defense Collaboration Services

DFARS —Defense Federal Acquisition Regulation Supplement

DIB —Defense Industrial Base

DISA —Defense Information Systems Agency

DoD —Department of Defense

DoDD —Department of Defense Directive

DoDI —Department of Defense Instruction

DoDIN —Department of Defense Information Network

DRU —Direct Reporting Unit

DSAWG —Defense Information Assurance Security Accreditation Working Group

DSS —Defense Security Service

DVD —Digital Versatile Disc

EIEMA —Enterprise Information Environment Mission Area

EITDR —Enterprise Information Technology Data Repository

eMASS —Enterprise Mission Assurance Support Service

EMSEC —Emission Security

EPL —Evaluated Products List

FAR —Federal Acquisition Regulation

FIPS —Federal Information Processing Standards

FISMA —Federal Information Management Security Act

FOA —Field Operating Agency

FOIA —Freedom of Information Act

FOUO —For Official Use Only

GIG —Global Information Grid

GWP —GIG Waiver Panel

HAF —Headquarters Air Force

HBSS —Host Based Security System

HIPAA —Health Insurance Portability and Accountability Act

HQ —Headquarters

HQ AETC —Headquarters Air Education and Training Command

HQ AFSPC —Headquarters Air Force Space Command

IAM —Information Assurance Manager

IAO —Information Assurance Officer

IAW —In accordance with

ICD —Intelligence Community Directive

ID —Identification

IMT —Information Management Technology

INFOCON —Information Condition

IPT —Integrated Process Teams

IS —Information System

ISSM —Information System Security Manager

ISO —Information System Owner

ISSE —Information System Security Engineering/ Engineer

ISSM —Information System Security Manager

ISSO —Information System Security Officer

IT —Information Technology

JP —Joint Publication

KMI —Key Management Infrastructure

KS —Knowledge Service

LRA —Local Registration Authority

MAO —Mission Area Owner (Component [AF] level PAO)

MAJCOM —Major Command

MFD —Multifunction Device

MICT —Management Control Internal Tool

MOU —Memorandum of Understanding

MPTO —Methods and Procedures Technical Orders

NC3 —Nuclear Command Control and Communications

NIPRNet —Non-Secure Internet Protocol Router Network

NIST —National Institute of Standards and Technology

NSTISSI —National Security Telecommunications and Information Systems Security Instruction

NSTISSP —National Security Telecommunications and Information Systems Security Policy

NTSWG —National Telephone Security Working Group

NSA —National Security Agency

NSA/CSS —National Security Agency/Central Security Service

NSS —National Security System

OMB —Office of Management and Budget

OPR —Office of Primary Responsibility

OPSEC —Operations Security

OSI —Office of Special Investigations

PAO —Principle Authorizing Official

PED —Portable Electronic Device

PEO —Program Executive Officer

PII —Personally Identifiable Information

PIN —Personal Identification Number

PIT —Platform Information Technology

PIV —Personal Identity Verification

PIV-I —Personal Identity Verification-Interoperable

PK —Public-Key

PKCS —Public-Key Cryptography Standards

PKI —Public Key Infrastructure

PM —Program Manager

PMO —Program Management Office

POA&M —Plan of Actions and Milestones

PPS —Ports, Protocol, and Services

PPSM —Ports, Protocol, and Services Management

RDS —Records Disposition Schedule

RMF —Risk Management Framework

SAAR —System Authorization Access Request

SACs —Self-Assessments Communicators

SAF —Secretary of the Air Force

SAISO —Senior Agency Information Security Officer

SAP/SAR —Special-Access Program/Special Access Required

SCA —Security Control Assessor

SCAR -- SCA —Representatives

SCI —Sensitive Compartmented Information

SCIF —Sensitive Compartmentalized Information Facility

SDLC —Software Development Life Cycle

SECAF —Secretary of the Air Force

SF —Standard Form

SIPRNet —Secret Internet Protocol Router Network

SISO —Senior Information Security Officer

SME —Subject Matter Expert

SME PED —Secure Mobile Environment Portable Electronic Device

SPO —System Program Office

SP —Special Publications

STIG —Security Technical Implementation Guide

STIP —Scientific and Technical Information Program

SVRO —Secure Voice Responsible Officers

SwA —Software Assurance

TAG —Technical Advisory Group

TDY —Temporary Duty

TMAP —Telecommunications Monitoring and Assessment Program

TO —Technical Order

TSCM —Technical Surveillance Countermeasures

UC —Unified Capabilities

UC APL —Unified Capabilities Approved Products List

UCDSMO —Unified Cross Domain Services Management Office

US —United States

USB —Universal Serial Bus

U.S.C. —United States Code

USCYBERCOM —United States Cyber Command

USSTRATCOM —United States Strategic Command

USM —Unit Security Manager

VoLAC —Volunteer Logical Access Credential

VPN —Virtual Private Network

VTC —Video Teleconferencing

WCO —Wing Cybersecurity Office

WIP —Workforce Improvement Program

WLAN —Wireless Local Area Network

Terms

AF CTTA —(Air Force Certified TEMPEST Technical Authority) An experienced, technically qualified government employee who has met established certification requirements according to CNSS-approved criteria (see CNSSP-300 and CNSSI 7000 (C/REL)), and is appointed by SAF/CIO A6 SISO to fulfill CTTA responsibilities. (AFMAN 33-286).

AFCTAG —(Air Force Cyber Security Technical Advisory Group) provides technical cybersecurity subject matter experts (SMEs) from across the MAJCOMs and functional communities to facilitate the management, oversight, and execution of the AF Cybersecurity Program. (See Figure 3.1).

AFIN —(Air Force Information Network) The globally interconnected, end-to-end set of Air Force information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy-makers, and support

personnel, including owned, leased and contracted communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (AFI 10-1701).

AFRMC —(Air Force Risk Management Council) Provides a forum for senior cybersecurity professionals to validate and vet issues concerning cybersecurity risk from a mission and business perspective. (See Figure 3.1).

ALT —(Alternate Logon Token) A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and to perform cryptographic functions. (AFMAN 33-282).

AO —(Authorizing Official) A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (CNSSI 4009).

ATO —(Authorization to Operate) The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (NIST 800-37, Rev. 1).

A&A —(Assessment & Authorization) (formerly C&A) The process by which organizations: (i) categorize information and information systems; (ii) select security controls; (iii) implement security controls; (iv) assess security control effectiveness; (v) authorize the information system; and (vi) [conduct] ongoing monitoring of security controls and the security state of the information system. (NIST 800-37, p. 4 *adapted*).

CND —(Computer Network Defense) Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. (CNSSI 4009).

CTO —(Cyber Tasking Order) An operational type order issued to perform specific actions at specific time frames in support of AF and Joint requirements. (AFI 10-1701).

Cybersecurity —(Information Assurance) Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (CNSSI 4009).

CYSS —(Cyberspace Support Squadron) Provides cyber networking expertise to AFSPC for Cyberspace Lead MAJCOM activities and functions.

DAMO —(Damage Assessment Management Office) Conducts damage assessments by collaboratively analyzing information compromised as a result of cyber intrusions to Defense Industrial Base information systems to determine overall impact to current and future Air Force weapons programs, scientific and research projects, and warfighting capabilities. (DoDI 5205.13, *adapted*).

DaR —(Data at Rest) Information that resides on electronic media while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated. Data at

rest can be archival or reference files that are changed rarely or never. Data at rest also includes data that is subject to regular but not constant change. (DoDI 8580.02-R).

DC3 —(Department of Defense Cyber Crime Center) Provides digital and multimedia (D/MM) forensics, cyber investigative training, research, development, test and evaluation (RDT&E), and cyber analytics for the following DoD mission areas: information assurance (IA) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT). (**https://www.dc3.mil/index/about-dc3**).

EIEMA —(Enterprise Information Environment Mission Area) IEMA is the DoD information (IT) portfolio that manages investments in the current and future integrated information sharing, computing and communications environment of the Air Force Information Network (AFIN). The IE comprises AFIN assets that operate as, provide information transport for, perform enterprise management of, and assure various levels and segments of the enterprise network, ranging from local area to wide area networks and from tactical to operational and strategic networks. The domains are Communications, Computing Infrastructure, Core Enterprise Services, and Information Assurance. (DoD CIO Memorandum, *Enterprise Information Environment Mission Area (EIEMA) Domain Owner Designations*, dated July 14, 2004).

EITDR —(Enterprise Information Technology Data Repository) EITDR is the Air Force IT Portfolio Management system of record. EITDR is accessible through the Air Force Portal. EITDR contains a current inventory of initiatives, systems, and system-related data and is used for internal management and oversight as well as to provide information to external sources to satisfy statutory and regulatory requirements. (AFI 33-141)

eMASS —(Enterprise Mission Assurance Support Service) eMASS is a government-owned, government-off-the-shelf (GOTS) web-based application, which supports cybersecurity program management. EMASS is fully compliant with security controls-based cybersecurity.

eMASS is designed to operate in either the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) enclave or the Secret Internet Protocol Router Network (SIPRNet) enclave. eMASS is public-key enabled (PKE) and all data in transit is fully encrypted. (**https://emass-airforce.csd.disa.mil/Content/Help/eMASS%205.1%20User%20Guide.pdf**).

ISO —(Information System Owner) Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (CNSSI 4009).

ISSE —(Information System Security Engineering/ Engineer) Individual assigned responsibility for conducting information system security engineering activities. (NIST 800-37).

ISSM —(Information System Security Manager) Individual responsible for the cybersecurity of a program, organization, system, or enclave. (CNSSI 4009)

ISSO —(Information System Security Officer) Individual assigned responsibility by the senior agency information security officer (SISO), authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (CNSSI 4009).

IT —(Information Technology) (A) The term "information technology," with respect to an executive agency means any equipment or interconnected system or subsystem of equipment,

that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(B) The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (40 U.S.C., Sec. 1401)

MAO —(Mission Area Owner) The person responsible for a defined area of responsibility with functions and processes that contribute to mission accomplishment. (DoDD 8115.01).

PED —(Portable Electronic Device) Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders. (ICS 700-1)

PIT —(Platform Information Technology) IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. (DoDI 8500.01).

RMF —(Risk Management Framework) A structured approach used to oversee and manage risk for an enterprise. (CNSSI 4009).

SCA —(Security Control Assessor) The individual, group, or organization responsible for conducting a security control assessment. (NIST 800-37).

Security Control Assessment —The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (NIST 800-37).

SISO —(Senior Information Security Officer) Official responsible for carrying out the chief information officer (CIO) responsibilities under the Federal Information Security Management Act (FISMA) and serving as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers. (CNSSI 4009).